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-

原田要之助[1]

概要

ITガバナンスは、コーポレート・ガバナンスのアナロジーから経営者が組織のITの投資や利活用について責任をもつ概念である。最初に、ISACAによって概念が提案され、オーストラリア・ニュージーランドの規格を経て、ISO/IEC385000の国際規格が作成された。その後、ビジネスへのコンピュータの利活用が進むにつれて、顧客情報などが漏えいする事件を引き起こすようになった。この問題も経営が関わることから情報セキュリティガバナンスが提案されて、ISO/IEC27014の国際規格となっている。日本では、情報セキュリティ報告書などにより情報セキュリティの状況が報告されている。企業によって大規模に集められたビッグデータについては、データの所有者との関係や分析への懸念から、制約や規制が必要になりデータガバナンスが提案されている。ビジネスでのIT利用が進むにつれて、経営者の関与が必要となった。今後のビジネスにはAIが高度に利用されるようになると考えられる。すなわち、今までのアナロジーからは、AIを利用する企業にはガバナンスが必要になると考えられる。本稿では、ITガバナンスの進展した経緯を振り返り、AIについてのガバナンスに必要性とその要件について述べる。

1 はじめに

ビジネスの効率化や正確性向上のために、企業では1960年代からコンピュータが広く使われるようになった。コンピュータの価格低下にともなって、企業では経営に関わる様々な情報をコンピュータで管理して日常の経営判断に繋げるようになった。コンピュータの利活用が進むにつれて、ビジネスの様々な場面において情報をデータとしてコンピュータに保存し、利活用するようになった。コンピュータのビジネスへの利用についてはマイケル・ポーターの競争の戦略などに取り上げられ、経営に有効であること、とくに企業競争力の源泉となることが認識されるようになった。しかし、ビジネスへのコンピュータ利用においては、負の側面が現れるようになった。コンピュータをビジネス

1 情報セキュリティ研究科　教授

に十分に生かすためにプログラムを開発する必要がある。また、コンピュータの運用には専門家が必要である。すなわち、企業のビジネスへのコンピュータの導入や利活用には、大規模な投資が必要であり、企業の経営に関わる問題であることが分かった。この問題については、コンピュータの企画、開発、導入、運用、廃棄の全てのライフサイクルに渡ってのコスト管理やプロジェクト管理が必要であることが議論され、企業の投資や経営を監視するメカニズムの必要性が認識されるようになった。これは、コーポレート・ガバナンスのアナロジーからITガバナンスとして知られるようになった。コンピュータへの投資が膨らむにつれて、この問題は経営にとって無視できないものとなった。システム監査では、システムへの投資や運用の効率化について分析する。しかし、投資や効率的な運用については経営の問題であり、マネジメント層ではなかなか解決できない。このような経緯から、ISACA（情報システムコントロール協会）から経営者がガバナンスする対象であるとするIT
ガバナンスが提案された[1]。

さらには、企業の重要な価値を持つ情報がコンピュータの内部にあることから、データを不正に利用するなり、窃盗するような事件が起きるようになった[2]。そのため、企業の情報セキュリティ対策が重要となった。さらには、情報セキュリティ対策には費用がかかること、外部に顧客情報が漏えいすると社会的なインパクトになることが分かり、企業の情報セキュリティにもIT同様にガバナンスが必要であることが認知されるようになった。これが情報セキュリティガバナンスである。米国では、民間主導で情報セキュリティガバナンスの必要性が提言された。

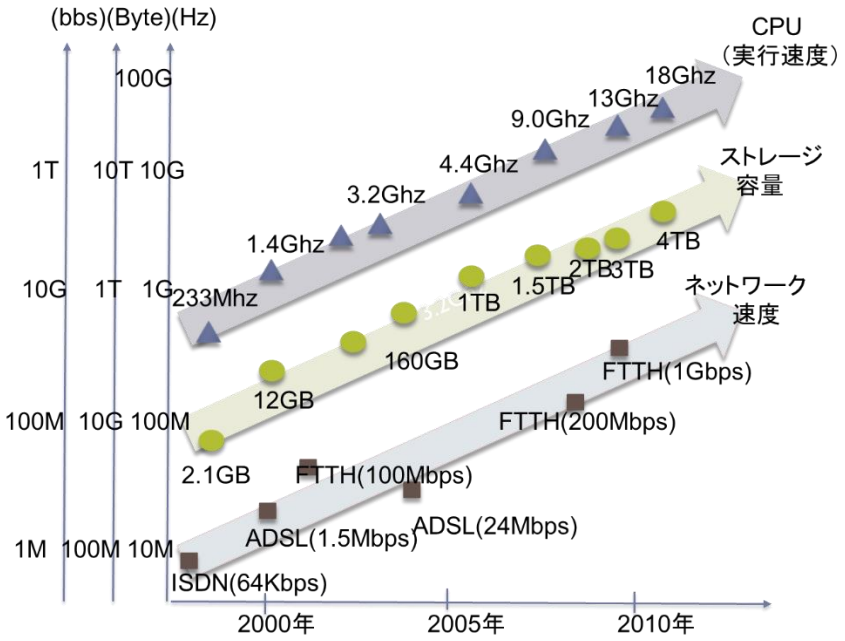

図1　コンピュータの能力、ストレージ、通信速度の進歩[3]

2000年代になって、コンピュータの能力がさらに大規模なデータの管理や大規模なデータ処理が可能となった。この進歩の状況を図１に示す。図１は、インテルの創始者の一人であるムーア氏が提言したムーアの法則[2]に従っていることが見られる。ムーアの法則では、プロセッサの能力が2.5年毎に2倍となることが知られている。この法則は、ムーア氏が提唱して30年経つ現在においても成り立つこと、さらには、コンピュータのみならずストレージや通信能力までもが法則にしたがっていることが分かる。

マーケッティングでは、顧客の消費動向などの調査や分析を一部のサンプリングされた情報をもとに統計的な処理が施して、分析して企業の価格や経営方針を判断する。サンプリングであることやデータ分析とデータの活用で時間差があることから、顧客の動向を正確に把握出来ず、機会損失につながっていた。2010年代には、図１のコンピュータやストレージの能力拡大によって、ビッグデータと呼ばれる全てのデータを直接分析する技術が活用されるようになった[3]。例えば、リアルタイムで顧客の購買履歴を顧客の属性データなどと関連づけて分析して、好みの商品を提供できるようになった。このことは、企業経営者にとっては顧客への効率的な販売が可能となった。一方、顧客にとっては、タイムリーに自分の欲しいものが提供されるという利点があるものの、このためにプライバシーに関わる情報までもが企業に提供されて活用されることになる。一方、自分のさまざまな個人情報が企業のビジネスに活用されることから、不安をもたらすこともある。とくに、2000年以降、大規模な個人情報の漏えい事故が起きるようになった。これらの事故は、その性質から、今後も起きると考えられる[4]。すなわち、ビッグデータの活用についても、情報漏えい対策のみならず、事後的に漏えいしたときの組織の対応なども考慮することが必要となり、データの対するガバナンスが必要であると考えられるようになった[5]。なお、図１の傾向から、レイ・カーツワイルらは、収穫加速の法則[3]に従って2045年にはAI（コンピュータ＋処理アルゴリズム）の能力が人間を上回るシングラリティ（特異点）が訪れると予測している[6]。すなわち、今後、コンピュータ、ストレージ、通信の能力が高まることから、今後本格化するAIについても同様なガバナンスが必要となる。

本稿では、2章にITガバナンスの経緯について述べる。企業の経営者がITガバナンスを実施するにあたって参考となるように規格ISO/IEC38500:2008[7]が策定されている。この規格の経緯と内容について論じる。3章では、ITガバナンスから情報セキュリティガバナンスへの流れと情報セキュリティガバナンスの規格であるISO/IEC27014について述べる。4章では、IT社会の中で個人に関する情報が収集され幅広くマーケティングに使われるようになった経緯と企業の経営者にとってデータガバナンスが必要となっ

---

[2] ムーアの法則については、学者の中でも見解が分かれている。技術的な限界から外れてきているというものと、巨視的な視点で見れば、他の技術がカバーして相対的には法則が維持されているという観点である。本稿では、文献[６]の立場にたち、今後もムーアの法則は継続するという立場をとる。

[3] 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 [6] 。

た状況とデータガバナンスの規格の特徴について述べる。5章では、今後、必要となるAIのガバナンスに関わる課題の所在と解決に向けたAIガバナンスについて提言する。

2 ITガバナンスについて

2.1 ITガバナンスの背景

コーポレート・ガバナンスの発展は、企業や組織 がゴーイングコンサーンを保証するために、事業に伴うリスクおよび株主価値の保護に関する透明性確保の必要性の観点から促進されてきた。これを実現する技術的な手段としてITを広範に用いるようになった。これが企業や組織のITへの大きな依存(エネブラとしてのIT)に繋がり、その結果として、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、ITを経営戦略やガバナンスの対象として考えなければならなくなった[1]。このようにITが企業の経営にとって重要であるとの認識は，企業に広まった．この現象をコーポレート・ガバナンスとのアナロジーでITガバナンスの概念として最初に導入したのはISACAである。ITガバナンスという用語と概念は，とくに，ITの投資やリスク管理で困っていた企業のCEOやCIOに受け入れられた。コーポレート・ガバナンスのアナロジーでITガバナンスを導入したことが企業に広く受け入れられるようになった原因でもある。なお、この概念は、ISACAが広く世界に喧伝したことから、システム監査やIT評価の関係者に知られるようになり、これを重視した米国やオランダの企業のCIOやCEOが活用するようになった[9]。また、ITガバナンスの重要性に気づいた国の中では、オーストラリアとニュージーランド（AS8500）、南アフリカ（KING Ⅲ）では自国のIT環境に適したITガバナンスのガイドラインを策定した。日本では、経産省がシステム管理基準にITガバナンスの概念が含まれていることから、システム監査の中で位置づければよいとの考えが主流であり、ITガバナンスに関する個別のガイドラインを策定することはなかった。日本では、2006年から日本ITガバナンス協会[4]がITガバナンスの普及と啓発を行っている。

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[5]。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[8]として日本の工業規格にもなっている。

この規格は 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

[4] ただし、ガイドラインを策定するのではなく、ISACA の IT ガバナンスに関するセミナーによる紹介と文献翻訳に限った活動を行っている。

[5] 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）。

あり、IT ガバナンスの 6 つの原則、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。このモデルを図 2.1 に原則を表 2.1 に示す。

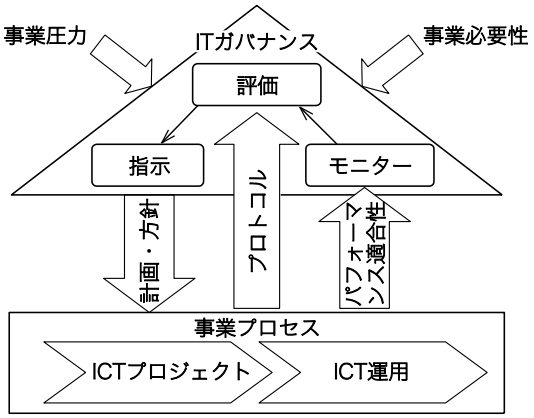

図 2.1 IT ガバナンスのモデル（JIS 38501:2014[8]より）

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ー、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（JIS 38501:2014 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ー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、網羅性も高い。

3 情報セキュリティガバナンスについて

3.1 情報セキュリティガバナンスの背景

ITガバナンスの出版のあと、ISACAは2003年に情報セキュリティについて、ITガバナンスのアナロジーから、情報セキュリティガバナンスを提言した［13］。これを機会に、米国のDHS（国家安全保障省）は民間企業と共同で2003年12月に米国のサンタクララにおいて、多数の専門家を集めてNational Cyber Security Summit[6]を開催した。このサミットでは、企業の情報セキュリティについて議論して情報セキュリティ対策の必要性について提言をまとめている。とくに、経営者の関与が必要として情報セキュリティガバナンスの重要性を提言した。これによって、米国では官民における情報セキュリティの重要性が認識されるようになった。日本においても、情報セキュリティの重要性が官民で認識され始めており、米国のNational Cyber Security Summitの動向に注目して、2005年から2010年まで情報セキュリティガバナンス委員会が開催されて、重要な情報セキュリティに関わる様々な検討が実施され、施策が打ち出された。

2.2 情報セキュリティガバナンスの規格ISO/IEC27014について

情報セキュリティガバナンスの国際規格は 2008 年に日本から ISO/IEC 及び ITU-T に対して規格化の提案がなされ、2013 年に ISO/IEC 及び ITU-T で国際規格化された。2008 年当時、ISMS（情報セキュリティマネジメントシステム）では経営者の関与が述べられているものの、具体的に経営層が情報セキュリティについてどのような取り組みをするかについては述べられていなかった。日本では、情報セキュリティガバナンス委員会で、ISO/IEC27001 の経営層が実施すべき内容として情報セキュリティガバナンスを ISO/IEC38500 のガバナンスをベースにまとめた［14］。これを国際の標準化の中で議論を深めて ISO/IEC27014 の規格となった。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 27014:2014[8]として日本の工業規格にもなっている。

[6] Information Security Governance: Call to Action (2004)として米国では、官民で情報セキュリティの重要性を共有した。

この規格は組織が情報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、ISO/IEC38500 と同様な 6 つの原則と情報セキュリティ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 3.1 に原則を表 3.1 に示す。

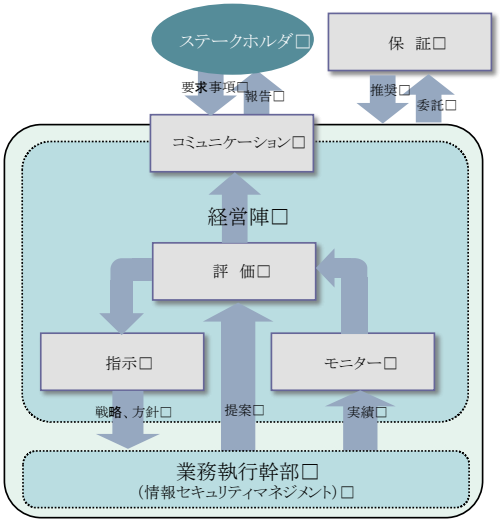

図 3.1 情報セキュリティガバナンスのモデル（JIS 27014:2014[8]より）

図 3.1 の情報セキュリティガバナンスのモデルは、IT ガバナンスと共通して組織の経営者が業務執行幹部による PDCA プロセスに対して実施すべき 3 つの機能であるモニター、評価、指示（EDM モデル）に、経営層がステークホルダに必要な情報を開示したり意見を聴取するコミュニケーションの機能と組織全体について監査したりする機能が追加されている。表 3.1 の情報セキュリティガバナンスの原則については、ISO/IEC38500 の原則と基本的な内容は共通しているが、記載については、文章となっている点が異なっている。ただし、内容で異なるのは，原則 2 にリスクが含まれている点である。情報セキュリティにとっては、リスクがベースとなってセキュリティ対策を考えるために必要である。なお、ISO/IEC38500 の責任に当たる項目が陽に述べられていない。例えば、情報漏えいの問題が起きたときの責任は組織の長にあることが自明であるためである。

表 3.1 情報セキュリティガバナンスの原則（JIS 27014:2014[8] より）

- 原則 1：組織全体の情報セキュリティを確立する。
- 原則 2：リスクに基づく取組みを採用する。
- 原則 3：投資決定の方向性を設定する。
- 原則 4：内部及び外部の要求事項との適合性を確実にする。
- 原則 5：セキュリティに積極的な環境を醸成する。
- 原則 6：事業の結果に関するパフォーマンスをレビューする。

4 データガバナンスについて

4.1 データベースの持つネットワークの外部性

個人情報がデータベース化された場合には、1章に述べたように、収穫加速の法則に従って、「多くの個人情報が集まるほどその効用が高まる」。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の重要な要素として、競争事業者間に広がる。そのため、業界として見た場合の個人情報のデータベース化がより広がっていくことになる。これは、IT化によるネットワーク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とこれを検索するときのコンピュータの処理能力が大きく影響する。さらに、通信速度の増加，コストの低下が加重する。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、利便性が増す。また、企業の多くではビジネスプロセスリエンジニアリングを実施して、省力化・無人化を図る。そのため、データベースを導入する以前の状態には戻れなくなり、データベースを管理することがビジネス上重要となる。多くの企業が、データベース化を図り、ビジネスに併せて拡大していく。これが、個人情報漏えいがなくならない要因となっている。

③ 顧客環境の変化

顧客においても、IT化が進んでいる。すなわち、パソコンやスマートホンなどの能力向上とコストの相対的な低下により、これらの機器を電子商取引に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。そのため、インターネットで個人情報などの情報を利用するケースが増大している。

以上の①～③による環境変化に伴う特性と、人間は情報処理に関する管理ミスや事故を確率的に起こすという習性を考慮すると、今後も、企業や組織においてデータベース化が進み、人為的な事件がなくならないと考えられる。

とくに，個人情報の場合、データの利用にネットワークの外部性が見られる[4]。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2倍以上となる。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。4.2節以降では、現在、標準化が進んでいるデータガバナンスについて規格の内容を紹介する。

4.2 データガバナンスの規格

ISO/IEC SC40 WG1 では、2 章で述べた IT ガバナンスをさまざまな分野に広げている。ここでは、ビッグデータに対するガバナンスを主たる目的として、データガバナンスを検討しており、規格化が進められている。規格の主要な目的は、組織の経営者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、収集した情報の活用、不要になったものの廃棄のライフサイクルを実施する）を導入しこれを活用・管理監督できようにするかである。なお、データのガバナンスの規格は。ISO/IEC SC40 WG1 の 2016 年 11 月会議で、FDIS 文書となっており、年内には最終案がとりまとめられ、2017 年には規格が出版される予定である。

本稿では、AI のガバナンスやマネジメントを考える上で参考になる部分について紹介するとともに議論する。

4.3 データガバナンスの規格の構成

データガバナンスの規格では、ISO/IEC38500 の IT ガバナンスの 3 章では良好な IT ガバナンスのための枠組み（原則とモデル）、5 章では 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 4.1 に示す。表 4.1 では、対象とするものが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 章で全体を俯瞰する構成となっている。

データガバナンスでは、IT や情報セキュリティなどのガバナンスの一般論と異なり、データをどのように扱うかなど、データ特有の項目を盛り込むことで、より実用的なガイドラインを目指している。

表 4.1 データガバナンスの規格案の構成（[20] より）)

3 Good Governance of Data
4 Principles、 Model and aspects for Good Governance of Data
5 Data Accountability

6 Guidance for the Governance of Data - Principles
7 Guidance for the Governance of Data - Model
8 Guidance for the Governance of Data - data-specific aspects
9 Application of the Data Accountability Map

4.4 データガバナンスの規格の自主規制について

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 章に「良きデータガバナンス」を設けて、経営者に対するデータを取り扱うときの心構えを述べている。これを、表 4.2 に示す。表 4.2 では、とくに、データ資産の適切な運用と多くの場合、ビッグデータでは、顧客の属性と組み合わせた付加価値の高いデータとなっていること。また、匿名性が求められているが、データの組合せによって個人が特定されるリスクもあることから、データの保護の重要性について述べている。さらに、データ解析によって、特定の顧客にとって有害な情報が得られるリスクもあることから、「有害な結果に繋がらないようにする」ことを求めている。これらの点については、ビッグデータに関わる問題点として取り上げられている基本でもある。これを強調している点が興味深い。

表 4.2　経営者に対する心構え（[20] より）

適切な「データガバナンス」は、経営者が以下の項目を通じて、組織全体でのデータ活用を進め、組織のパフォーマンスに寄与できるようにする。
①　サービス、マーケット、ビジネスにイノベーションをもたらす
②　データ資産を適切に導入して運用する
③　データの保護と付加価値の可能性の両方に対する責任と説明責任を明確にする
④　有害で意図しない結果につながることを最小化する

表 4.2 はビッグデータを用いる際に企業には様々な制約があることから、この規制面だけでは規格としてバランスを欠くので、このデータのガバナンスを経営者が実践することで何が得られるかについても表 4.3 に述べている。データガバナンスによって経営者には、様々な価値がもたらされるとことが分かる。このような自主規制やメリットについては ISO/IEC38500 にはないもので、データの特性からくる新しいガバナンスの側面をより理解できるように設けられたものである。

表 4.3　データのガバナンスによって得られるもの（[20] より）

データガバナンスを実践できている組織は以下のような組織である

① データのオーナーとデータの利用者が取引できる信頼のある組織
② データのシェアについて信頼を提供する
③ データの知識財産やその他の付加価値に対する保護
④ ハッカーや不正行為を抑止するポリシーを持っている
⑤ データの漏えいの影響を最小限にできる備えを持つ
⑥ データの再利用についての認識がある
⑦ 良好なデータの取扱について外部に見せることができる

規格では、さらに、「良きデータガバナンス」がない場合のリスクについても記載している。これを表 4.4 に示す。表 4.4 のリスクには、データに関する法制度とデータ漏えいリスクが述べられている。

表 4.4　データガバナンスがない場合のリスク（[20] より）

この規格では、データガバナンスのためのモデルを確立します。原理を適切に適用したモデルを利用することによって、自分の義務を果たしていない経営者のリスクを軽減できる。なお、データのガバナンスが不十分な場合には、組織は次のようなリスクにさらされる

- 法制度に準拠していない場合の罰則– 特にプライバシー対策に関連した法制度
- ビジネス・データの機密性の損失、例えば、製法や設計仕様、
- ビジネスパートナー、顧客、一般を含むステークホルダからの信頼の喪失、
- 信頼できるビジネス関連データの不足のために重要な組織機能を実行できない
- 競合他社がデータを戦略的活用することで競争が激化する

4.4 データガバナンスの原則について

データガバナンスの規格における原則（Principles）を表 4.5 に示す。ISO/IEC38500 の 6 つの原則をそのまま適用していることが分かる。ちなみに、IT のガバナンスとデータのガバナンスについて、同じ 6 つの原則が当てはまるか、また、不足する原則があるのではないかについて標準化の中で深く議論された。さまざまな見解があり、例えば、リスクについて原則を設けてはとの意見もあった。しかし、リスクについては経営者の経営判断の中で実施するものであり、リスクマネジメントについては ISO31000 で規格化されており、これに追加するものがないこと。経営者は IT ガバナンスの規格とリスクの規格の両方を用いて判断するのがよく、ここにリスクを書くと両方の規格でリスクを扱うことになり、却ってリスク対策について責任や対応が不明確となることから、データのリスクについても

IT ガバナンスと同様に ISO31000 を用いればよいとの結論となった。最終的には、データガバナンスの原則は、 6 つの原則で十分である。

表 4.5 データのガバナンスの原則（[20] より）

- 6. 1 General
- 6. 2 Principle 1 - Responsibility
- 6. 3 Principle 2 - Strategy
- 6. 4 Principle 3 - Acquisition
- 6. 5 Principle 4 - Performance
- 6. 6 Principle 5 - Conformance
- 6. 7 Principle 6 - Human Behaviour

4.6 データガバナンスのモデルについて

データガバナンスでは、 2 つのモデルが図示されている。データのライフサイクルをベースにしたデータのマネジメントモデルを図 4.1 に示す。また、これを経営者がどのようにガバナンスするかの EDM モデルを図 4.2 に示す。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が述べられている。

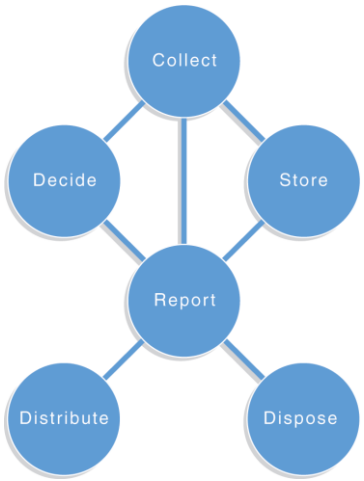

図 4.1 データマネジメントモデル（[20] より）

図 4.2 は、ISO/IEC38000 のモデルである図 2.1 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。図 4.2 のデータマネジメントモデルでは、プロセス毎に経営者が果たすべき EDM 機能が述べられており、図 2.1 の EDM モデルがベースとなること、機能面で過不足がないことが述べられている。

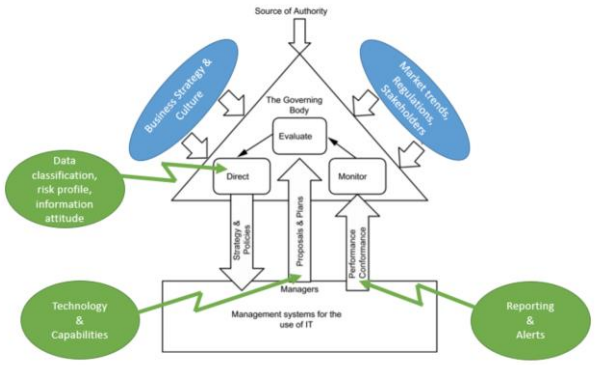

図 4.2 データガバナンスモデル（[20] より）

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

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、モニターについても経営者目線で記載されている。一方、データガバナンスでは、データのオーナーが企業内部とは限らないため（例えば、顧客情報など)、また、個人情報を入手するためには、対象者から収集にあたって同意をとる必要がある。すなわち、データガバナンスでは、内部のプロセスを経営者が内部的にチェックするだけではステークホルダへの説明責任として十分ではない。そこで、データガバナンスの規格化にあたっては、内部のガバナンスを外部に担保するための追加的な機能が必要としている。この章として、「経営者と監視機構（Oversight Mechanism)」を設けている。この内容を表 4.6 に示す。表 4.6 では、経営者がデータの取扱について十分な注意義務を果たすべき事、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、より、厳しい経営者の監督義務を課している。

表 4.6 データの経営者と監視機構について（Oversight Mechanism）（[20] 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ーする必要がある**

① 個人情報とITの関係

個人情報のIT化について検討する。個人情報は、ITが普及する前からビジネスの有効なツールであった。しかし、個人情報の活用が脚光をあびるようになったのは、ITが利用されるようになった1970年代以降である。さらに、1990年代には、パソコンの能力向上とコスト低下にともなって、より広くビジネスにITが利用されるようになった。そのため、ビジネスでは、ITを利用した個人情報の集積が進み、広く利用されるようになった。

② 個人情報のデータベース化

次に、個人情報がITを利用してデータベース化される誘因について考えてみる。個人情報をビジネスで利用するのは、主に顧客へのプロモーションとアフターサービスである。プロモーションの場合には顧客に関する属性情報をもとに売り込む商品を決めたり、新しい商品のコンセプトに合う顧客を検索したりする。紙ベースで顧客情報を管理している場合と比べると、効果が高い。一方、アフターサービスでは、顧客からの問い合わせに対してタイムリーに対応することで顧客満足度を高め、顧客を囲い込むことができる。具体的には、顧客に販売した製品が何で、いつ販売したのか、その履歴はどうなのかなどが個人情報と併せてデータベース化されるようになっている。また、販売した後にも、顧客に問いかけて製品の状況や不満などを聞くことができる。すなわち、個人情報の活用がビジネスの鍵であり、顧客の個人情報をITで管理できることで、顧客を囲い込むツールがより強化される点が大きな誘因となる。すなわち、個人情報のデータベース化は、ビジネスの観点からみると大規模化に向かうと考えられる。

③ 個人情報の漏えいの管理

個人情報は、①に述べたようにビジネスの有用なツールであるため、利用される頻度が高い。また、個人の情報は時間とともに変化するため、個人情報保護法への準拠のため、事業者は常にデータベースのアップデートが必要である。また、同意を得て関連会社などに利用させるようなケースもあり、管理が十分でないケースも起きる。

さらに、②に述べたように、データベースの外部性を認識できず、規模に応じた管理ができず従来通りの管理にとどまることが多い。しかし、競争環境下では、競合相手にとっても大きな価値を持っているため、個人情報自体が価値を持ち、ブラックマーケットでは、高く販売される。そのため、大規模な個人情報の漏えいのリスクも高まる。企業の経営者は、この特性に注意してガバナンスすることが重要であり，ISO/IEC38505［20］が活用されることになると考えられる．

5 AIのガバナンスについて

5.1 AIの特性から

ダベンポートは、AI の能力を 4 つの発展段階でまとめている［15］。これを筆者の観点で見直したものを表 5.1 に示す。なお、表 5.1 の横軸は作業を、また、縦軸は、AI が実施する内容を示す。縦軸の上から、アルゴリズムの進展が高度化する。ちなみに、第 3 段階はデジタル作業を示し、第 4 段階は、アルゴリズムを示す。一方、表 1 の横方向は、学習能力を 4 つの発展段階で示している。人間が利用する、第 2 段階では反復する作業を自動化する。ただし、AI が経験や状況の変化に応じて作業結果をパラメータなどの形で取り込むことで個別の環境に対応する。これらのパラメータは人が与え、選択する。AI が自動で選択する場合もある。これが進んだ第 3 段階では、AI が自らの作業効果や分析結果を人の介在なく観測することができて、これまでに蓄積した知識を用いるとともに、環境に適合しない場合には、修正する。ただし、パラメータなどは自由に操作できるが、操作手順などのアルゴリズムについては修正することができない。第 4 段階では、環境を自己認識できてアルゴリズムが良くない場合には、アルゴリズム自体を自己で修正できる

なお、表 1 の縦軸と横軸に対応する、現在実現できているものが示されている。なお、表中の「未」はまだ、技術が開発されていないことを示す。ダベンポートは、学習能力の第 4 段階については、フィクションの世界と言いつつ、AI が自己を認識する知性を持つ段階としている。この段階では、AI が自分で目標を検討して、それに至る別の解を見つけるとともに、目標自体についても、設定がおかしければ疑問視するようになると述べ、現状では、この段階のものは存在しないとしている。なお、表 1 にはダベンポートの提案に追記する形で、新しい技術を追記している。例えば、FinTech やスマートハウス、ワトソンやアルファ「碁」など最新の話題を網羅した。

表 5.1　認知テクノロジーの種類とその進化（［15］に加筆修正）

作業の種類	人間支援	反復作業の自動化	状況認識・学習	自己を認識した知性
数値分析	データ分析 ビジネス・インテリジェンス、データの可視化	オペレーショナル分析、自動採点、モデル管理	機械学習、ビッグデータ解析、	未
言葉や画像の理解	文字や音声の認識、文章推敲型ワープロ	画像認識（顔認証）、VR（仮想現実）	ディープラーニング、IBM ワトソン、アルファ「碁」	未
デジタル作業の遂行	ビジネスプロセスの管理、自動倉庫、受発注のオートメーション	ルールエンジン、自動検索エンジン、製造プロセスの自動化、FinTech	未	未
物理的作業の遂行	工場などの装置の遠隔操作	産業ロボット、介護ロボット、監視システム	自立走行ロボット、自動運転車、スマートハウス	未

表 5.1 は、AI のアルゴリズムが人の手を支援する段階から、学習して判断する段階を経て、自己を認識した知性を備えた段階に進むことが示されている。また、作業内容としては、コンピュータの得意な数値処理から始まり、言語や画像の認識、人が実施してきた作業を実施する。段階が進むにつれて、AI の利用が高度化する。すなわち、ブルーカラーの分野における労働力の置き換えから、専門的なホワイトカラーの分野における専門職の置き換えにつながることである。

5.2 AIの参照モデル

AI を検討するにあたりモデルを想定すると理解しやすい。本稿では、金子による参照モデル［19］を用いる．これを、図 5.1 に示す。

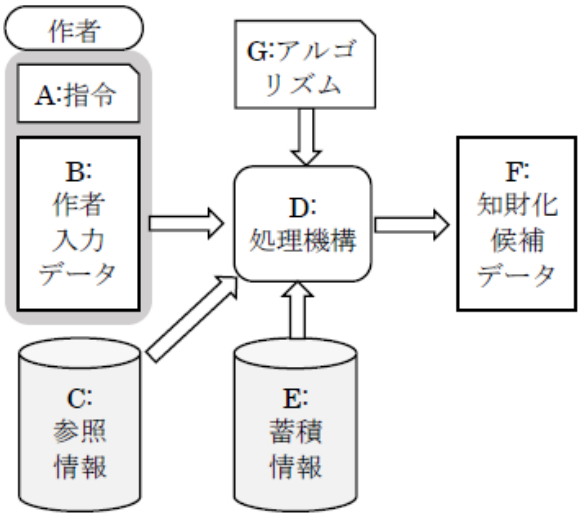

図5.1　AIのリファレンスモデルについて　出所：[19]

図 5.1 のモデルでは，情報処理を行う AI は、２つの概念的なデータベース（図中 C と E）のデータを処理する機能（図中の D）から構成される。C のデータベースはインターネットで接続されて公開された一般化されたデータであり，データを容易に収集し，加工することができるものの総称である。C のデータについては公開されたものでありオンラインとオフラインの世界中の全てのデータを含む。人類が長い歴史の中で集めた全てのデータであり、無料若しくは安価な対価で入手できる。一方 D のデータベースは、AI のシステム内部に蓄積されたデータであり、これは外部から購入したものや自分で収集したり作成したりしたものを指す。すなわち、D のデータベースの所有権は自分にあり、自由に利用できる。これらの二つのデータベースから処理機構としての AI は新しい知識を発見したり著作したりすることが可能なモデルである。

5.3 外部参照情報の課題

図 5.1 のモデルでは，AI が C で示す外部の参照情報を用いて新しい発明や著作を行う行動を模式化したものである。すなわち、人が Web や書籍などの公開情報を用いて創作や企画を作成する場合の行動をモデル化している。このモデルはネットワークが発展している現在のモデルのように見えるが、ネットワークの発達していない時代には情報や知識が集積された図書館などに出向いて活用していたので、人間の創造の普遍的なモデルと考えることができる。ただし，このモデルでは、データベースを単純化しており、生のデータ（測定データのように得られたデータなど）、情報（データに意味づけを与えて，利用できるようにしたもの）、知識（情報を活用して得て，法則や原理などに結びつけたもの，後生に残すための記録など）の区別がなされていない。生のデータについてはデータの所有権、情報については分析や付加価値についての権利（著作権など）が発生する。さらに、知識については、その考案したものや発明についての権利（特許など）が発生する。

本稿では、上記の生のデータ、情報、知識を区別せずに知財オブジェクトとして扱う。このオブジェクトは，さまざまな権利関係に紐付いたオブジェクトが連携したものである。一般に公開されているデータや情報についても、利用するための条件が科せられているものもある。

C についてはビッグデータなどで議論されるにつれて、データに対する権利面での課題や個人の行動情報や位置情報などデータの所有者との関係でデータの活用の際に許諾が必要になるなど，さまざまな社会的な課題が提起されている。すなわち、C については，例えば、社会公共的な理由をもとに、AI が自由に使えるようにするには課題が多い。

とくに、AI が C を用いて収益活動するようになったときには、例えば、膨大な情報を無料で活用し、その成果を独り占めすることになると考えられる。そのため、フリーでアクセスして活用出来るための社会的なインフラのコスト負担についてバランスしなくなる可能性がある。この問題については、今後、解決していく必要がある。例えば，現在，音楽のように多数の利害関係者が関わるコンテンツ（データと区別するために，このように述べる）については、著作権を JASRAC に一元化して徴集して関係者に配分するしくみなどが必要になると考える。

5.4 AIの処理機構の課題

図 5.1 のモデルでは、AI の知的な活動の部分として D の処理機構が述べられている。今後，AI の能力が加速度的に進歩して人間の能力を超えることが懸念されている［2］。とくに、能力が飛び抜けた存在する中で、対等にビジネスをした場合に、能力を持たないものとの間で格差が広がる。

この問題点の例として、株式の高速処理およびアルゴリズム取引の不公平さをあげることができる。現在の証券取引所は，注文を受け付ける時間は 2000 分の 1 秒以下となっていて、大手の銀行や証券会社が高速なコンピュータを用いて“高頻度取引”を実施している。一般のパソコンやインターネットを利用したデイトレーダーのような小規模な投資家はこ

のような高速な取引を有効に活用できない。結果として、高速な取引に加われないために機会損失を受ける。最悪のケースでは、高速取引の餌食になる可能性もある。また、高速取引は、一つのミスを拡大して巨額の損失につながって市場に悪影響を与える。米国では、既に事件が起きており、様々な規制が実施されている[]。

AI の能力が拡大して、株の取引を行ったときに、AI を持つ者と持たざるものとの格差が広がり、株式市場を破壊してしまう懸念がある。グローバル経済はお互いに繋がっているため、一つの AI のミスが世界恐慌を引き起こす可能性がある。

5.5 AIのアルゴリズムの課題

図 5.1 のモデルでは、AI のアルゴリズムを G に表現している。5.1 節に述べているように、ダベンポートは、AI が自己を認識した知性の段階に至る段階ついては、人と AI の間で雇用問題が起きて、人を除外することにもなるため、AI の開発や適用領域について何らかの制約が必要になると述べている。今後、AI は様々なアルゴリズムを完備するようになり、より人間に近い能力を代弁していくことになる。当然、人のような社会的な制約やモラルが求められる。これには、ロボット 3 原則のようなものが必要となると考えられる。

なお、我々の社会生活の場面では、全ての物事を 0 と 1 で決めきれない。グレイなままで済ませることがある。これらは、ときには、論理的でないばかりか、矛盾した判断を下すことがある。これを身につけるためには、人は長い教育を受けて、IQ のみならず EQ を身につけている。前者にとって言えば、世の中野理論を学び、後者にとって言えば、世の中の矛盾した現実を知るために様々な人と議論したり、分析したりして、問題をどのように解決するか、曖昧なままで済ませることなどを教養として身につけている。AI にこのような教育を施すことが可能であろうか。今後、この問題を AI のガバナンスに取り込む中で検討していく必要がある。

4 章に述べたビッグデータについては社会的な関心の高まりから、データに関するガバナンスが議論されるようになった。AI についても、2 章に述べてきたように，同様な問題があり，社会的な関心も高まっている。すなわち、データ同様に AI についても早急にガバナンスを検討すべき時に来ていると考えられる。次節では、4 章に述べたデータのガバナンスを参考に、AI のガバナンスを検討する。

5.6 AIのガバナンスについて

5.1 節から 5.5 節まで、AI の特徴について検討した。以上の検討からは、AI についても AI を導入する企業や組織がガバナンスすることが求められることが分かった。また、コーポレート・ガバナンスから IT ガバナンスや情報セキュリティガバナンスに発展した経緯や企業や組織がその技術を導入して問われるべき社会的な責任は、IT、情報セキュリティ、データと範囲が拡大している。IT では、導入は経営判断で十分であるが、投資効果があるのか、ビジネスに与える影響など限定されていた。情報セキュリティでは、企業に所有権

のない顧客に関する個人情報などを収集してビジネスに利用することから、情報に対する管理すなわち、情報セキュリティに対する責任が発生する。大規模な情報漏えいでは経営者がお詫び会見を実施するのは、企業の責任を超えているためである。そのために、個人情報などの取扱についての情報開示や監査が必要となっている。ビッグデータについても、情報セキュリティと同様な部分があるが、企業が取得したり自分のビジネスの中で収集したりしたデータについて他のデータと関連づけたりして分析をどこまで実施できるかが重要な課題となっている。この部分については、法的に曖昧な部分があり、企業の自主規制に委ねられている。また、データが国境を越えて広くクラウドなどに分散することもあり、そもそも、一国の規制でカバー仕切れない。そこで、データガバナンスが一つの自主規制をガイドするものとなっている。

AI についても、データガバナンスと同様な問題があり，AI を所有してビジネスに活用するのは企業や組織の自由である。ただし、5.1 節や 5.5 節に述べたように、AI については将来的に人間の能力を超えることが予測されており、今後、社会に対して問題を引き起こす可能性が指摘されている。これには、ロボット原則などがあり、今後の研究が待たれる分野である。また、5.5 節に述べたように AI を持つ者と持たざるもので社会・経済的な格差が拡大して不公平な社会となることも懸念されている。これらのことから、まずは、AI についても早急にガバナンスを検討すべき時に来ていると考えられる。

AI のガバナンスをコーポレート・ガバナンス、IT ガバナンス、情報セキュリティガバナンス、データガバナンスが生まれた経緯やガバナンスの対象、タスク、原則などについて比較検討した。これを表 5.2 に示す。表 5.2 の各項目を比較すると、ガバナンスの主体は経営者であるものの、ガバナンスを要請する側は、ステークホルダから、データの所有者、AI では社会へと広がっている。この特性に合わせてタスクや原則が対応することになる。これらのことから、AI のガバナンスについては、タスクや原則について、より対象を広げたものが必要となると考えられる。表 5.2 では、アナロジーから、AI のガバナンスのフレームワークが、IT ガバナンスの 6 つの原則だけでは十分でないことが分かる。すなわち、社会が関わる例えば、ロボット原則（AI を社会が規範として制約できるしくみ）が必要である。本論文では、AI についての一般論をベースに他のガバナンスからのアナロジーとして、AI についても AI ガバナンスが必要であることを提言した。しかし、まだ、AI の能力や倫理の適合性などの検討が不十分であり、AI ガバナンスについてさらなる検討が必要である。

表 5.2　ガバナンスの比較

	ガバナンス主体とガバナンスの対象	タスク	原則	形態
コーポレート・ガバナンス	経営者 ステークホルダ	経営者の一般的な義務	あり	企業の努力義務

IT ガバナンス	経営者 ステークホルダ	EDM モデル （評価や監査は別の規格）	６つの原則（責任，戦略，取得，パフォーマンス，適合性，人間行動）	企業の努力義務
情報セキュリティガバナンス	経営者 ステークホルダ	EDM モデル＋コミュニケーション，監査	６つの原則（責任，リスク，取得，パフォーマンス，適合性，人間行動）	企業の努力義務
データガバナンス	経営者 データオーナー （社会）	EDM モデル＋データマネジメントモデル	６つの原則（責任，戦略，取得，パフォーマンス，適合性，人間行動）	企業の努力義務
AI ガバナンス	経営者 ステークホルダ＋社会	EDM モデル＋AI マネジメントモデル	６つの原則（責任，リスク，取得，パフォーマンス，適合性，人間行動，ロボット原則）＋倫理	企業の努力義務 ＋ 社会的な規範

まとめ

本稿では、企業などの組織の IT の活用に関わる経営者の責任問題がコーポレート・ガバナンスのアナロジーから始まった歴史について述べた。IT の投資や利活用の問題としての IT ガバナンスは、企業などの組織の情報セキュリティに関する経営者の責任問題としての情報セキュリティガバナンス、ビッグデータの活用に関するデータガバナンスに発展した。IT の最終的な形態である AI については、企業や組織において活用が始まったばかりであるが、社会に与える影響は極めて大きいことや、今までの IT ガバナンス、情報セキュリティガバナンス、データガバナンスとの共通性やアナロジーから、AI についてのガバナンス問題があることを指摘した。その解決策には、企業や組織においてAIの本格的な利用が始まる前にAIガバナンスを準備しておく必要であることを提起した。なお、本稿では、AI ガバナンスについての必要性と概念を示しただけであり、今後、実際の企業や組織を対象にしてより具体的な内容を検討する必要である。

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］取締役会のための IT ガバナンスの手引、ISACA、第 2 版、2003年
［２］NPO日本ネットワークセキュリティ協会、2015年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～、2016年8月

［３］岩本敏男、IT幸福論、東洋経済新報社、2013年
［４］原田要之助、大規模な情報漏えい事件の特性と対策の考え方、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. 186-198、2014年11月
［５］原田要之助、IPSJ SIG Technical Report、Vol.2016-EIP-73, No.7、2016年9月
［６］レイモンド・カーツワイル、スピリチュアル・マシーン コンピューターに魂が宿るとき，田中三彦・田中茂彦訳、翔泳社、2001年
［７］ISO/IEC、 ISO38500:2013、 Governance of IT、2013 年（オリジナルは 2008 年）
［８］日本規格協会、JIS Q38500:2014（ITガバナンス）、2014 年
［９］Rinnooy Kan, Information systems control journal, Information System Control Journal, V.2, 2004
［10］ISO/IEC、 ISO27014:2013、Governance of IT Security、2013 年
［11］日本規格協会、JIS Q27014:2014（情報セキュリティガバナンス）、2014年
［12］ISACA、日本規格協会、JIS Q27002:2006（情報技術―情報セキュリティマネジメントの実践
のための規範）、2006年
［13］ISACA、情報セキュリティガバナンス：取締役会と執行役員のためのガイドライン、第 2 版、2003年
［14］経済産業省、情報セキュリティガバナンス研究会報告書 - 情報セキュリティによる企業価値創造に向けて -、2007年
［15］トーマス・H・ダベンポート、ジュリア・カービー、AI 時代の勝者と敗者、 2016 年
［16］ISO、 ISO31000:2009、 Risk Managemeent - Principles and guidelines、 2009
［17］原田要之助、企業に求められる IT ガバナンスの新しいモデル、InfoCom REVIEW、情報通信総合研究所、vol.47、pp2-15、2009 年
［18］鈴木宏幸、新原功一、原田要之助、大規模な個人情報漏えいの特性を考慮した事業継続対策について、システム監査学会誌、Vol.27、2014 年 4 月
［19］金子格「AI, ML の産業応用の拡大における知的財産の扱いに関する考察」, IPSJ SIG Technical Report、Vol.2015-EIP-69, No.8、2015 年
［20］ISO/IEC FDIS 38505-1, Governance of Data、(2016 年 11 月現在)