プライバシー規制の強化や有事対応に対するInformation Governanceの有効性について

EY 新日本有限責任監査法人 Forensics 事業部マネージャー
公認不正検査士　池上　弘樹

1. はじめに

クラウドサービスの浸透やデジタルトランスフォーメーション（以下、DX という）の推進により、企業の保有するデータ量が加速度的に増加している一方で、2018 年に施行された「EU 一般データ保護規則（GDPR：General Data Protection Regulation）」を契機として、主なものだけでも米国カリフォルニア州、日本、インド、ベトナムなどのアジア諸国、ニュージーランド、ブラジルなど個人情報保護法の制定や強化の動きが加速しており、有事に企業が求められる対応は厳格なものへとシフトしています。インシデント発生時の混乱の中、ルールで定められた期限内の対応と適切な情報開示と通知を行うことは非常に難しくなっており、対応不備による規制当局からの制裁金や訴訟を回避するためにも、有事対応への備えとしての Information Governance（以下、I.G. という）の必要性が増しています。本稿では、この I.G. の概要と有事を見据えたリスク低減の例について解説を行います。

2. Information Governanceとは

Information Governance という言葉は広い意味で使われることが多いですが、一般的には企業や組織が保有している全ての情報をコントロールし、様々なリスクを低減した上で、適切なデータの利活用を促進し、企業の成長や戦略に利用するための枠組みや取り組みであると言えます。

今日の企業が抱える情報資産は、顧客データ、業務データ、財務データなど多岐にわたります。IT ハードウェアの進化、企業の DX 推進に伴うデータ量の爆発的な増加で得られる新たな石油[1]ともいわれる情報資産は、企業にとっては上手く活用すれば企業戦略の要となる一方、取り扱いを間違えると、致命的なリスクにもなると言えます。こうしたリスクを低減するためには、それぞれのデータやシステムに対して、適切なポリシーを適用し、対応措置（ガバナンス）の仕組みを確立し、コントロールすることが求められます。これにより適切で効率的なデータ活用が可能になり、持続可能な経営戦略を構築していくことが可能になります。デジタル技術による社会、競争環境の変化がもたらす影響（リスク・機会）を踏まえた経営戦略の策定は、昨年経済産業省が発表した、“デジタルガバナンス・コード”[2]でも柱となる考え方とされており、どの企業にとっても今後取り組むべき課題と言えます。

3. Information Governance Reference Model

Information Governance Reference Model（以下、IGRM という）[3]は、アメリカの任意団体、Electronic Discovery Reference Model[4]（以下、EDRM という）が策定した、I.G. についての参照モデルであり、その目的は、企業や組織が効果的かつ実用的な I.G. プログラムを実装するための、柔軟なフレームワークを提供することです。IGRM は、EDRM フレームワークの情報管理の部分にフォーカスし、構築するだけが目的ではなく、データ管理、コンプライアンス、IT インフラなど組織を横断的に管理する拡張可能な概念になります。

I.G. について何かから手を付けていいのかわからない、もしくは組織が現在どの程度 I.G. について

[1] Robert F. Smallwood：Information Governance　-Concepts, Strategies and Best Practices. P.5

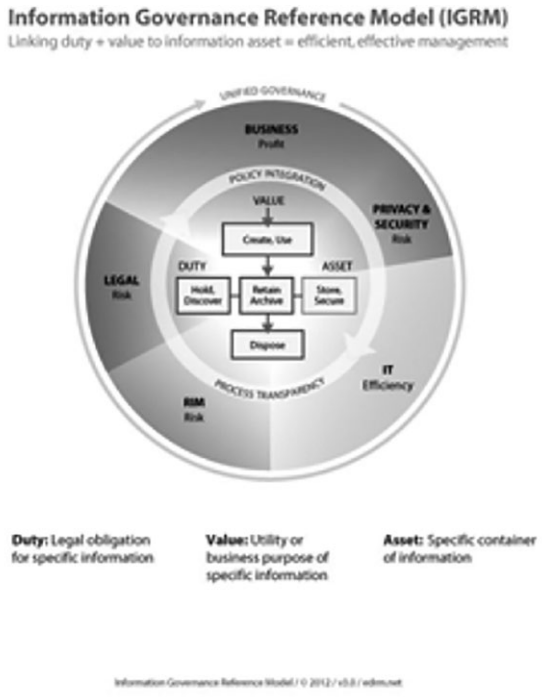
[2] https://www.meti.go.jp/shingikai/mono_info_service/dgs5/pdf/20201109_01.pdf

[3] https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

[4] https://edrm.net/
EDRMは、弁護士、裁判官、社内弁護士、その他の法律専門家、eDiscoveryベンダー等で構成され、電子情報開示、プライバシー、セキュリティ、および情報ガバナンスを向上させる実用的なグローバルリソースを作成しており、国際的な指標となっています。

取り組みが出来ているかを評価する意味でも、この参照モデルは有効に活用できます。また、IGRMは法務やITだけが活用するものではなく、この図をハブとして、経営層から各部署に渡り、横断的コミュニケーションを促進することを推奨しています。

この図が表現している通り、常にデータプライバシーやセキュリティの最新状況に配慮し、規定を最新の状態に保ち、保持しているデータの整備を実施し続けるサイクルを回し続けることが成功するI.G.の体制と言えます。



[5] Information Governance Reference Model（IGRM）

アメリカの市場調査会社、International Data Corporation（IDC）が2020年5月に行った発表によると、今後3年間に作成されるデータ総量が、過去30年間に作成されたデータ総量よりも多くなり、過去5年間で作成されたデータの3倍以上のデータが作成されるとしています。[6]

データ量の爆発的な増加の背景として、企業のDX　推進、5G、ブロックチェーン、AR（拡張現実）/VR（仮想現実）、AI/ 機械学習、IoTなどのテクノロジー、またここ1年間はコロナ禍の中、動画ストリーミング量の増加や、企業が在宅勤務を推進した結果、データ通信量が増えたことも影響していると言えます。

この爆発的なデータ量の増加に伴うリスクの増大に企業は対応することが求められます。保有するデータをいかに管理し、統制していくか、つまりI.G.の構築、実現は、企業にとって急務であると言えます。

4. Information Governanceが求められる背景 ーリスクへの対応ー

前項で述べたデータ量の爆発的増加に加え、贈収賄や談合（カルテル）などの法令違反リスク、情報漏洩や不適切会計などの不正リスク、海外当局調査や訴訟などの法的リスク、GDPRを始めとしたデータプライバシー規制への対応など、企業は様々なリスクへの対策と有事対応を求められます。

こうしたリスクへの対策の一例として以下の5点を紹介します。

・データマッピング
・重複・古いデータの戦略的削除
・文書管理規定の見直しとアップデート
・データ抽出方法の確認
・データプライバシー規制への対応

[5] https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

[6] https://www.idc.com/getdoc.jsp?containerId=prUS46286020#:~:text=08%20May%202020-,IDC's%20Global%20DataSphere%20Forecast%20Shows%20Continued%20Steady%20Growth,Creation%20and%20Consumption%20of%20Data&text=By%202024%2C%20IDC%20expects%20this%20ratio%20to%20be%201%3A10

今回紹介するこれらの対策はあくまで１つの例であり、各組織や業界の実情などを鑑みたリスクに応じて、対策を検討することをお勧めします。

4-1．リスクへの対応：データマッピング

I.G. への取り組みのスタート地点として、まず組織内のデータの現状を把握することは非常に重要です。データの種類の把握（構造化データ、非構造化データ、紙文書など）、データ量の把握をシステム別、本社、子会社、海外子会社別に実施することで、組織内のデータの状態を視覚化し、現状の問題点の特定や各データやシステムの責任者の明確化、リポートラインの確立など様々な行動をとることが可能になります。

データプライバシー規制への遵守状況もここで確認できます。自社のデータが格納されているサーバはどこにあるのか、そして国内外からのアクセスを含め、誰がどこからアクセスできるのか、この点は非常に基本的な事ではありますが、全てを把握できている企業が多いとは言えないことは、昨今の報道されている事案などから明らかです。
また、企業が M&A を実施した際のシステム統合や新たなソフトウェアの導入といったイベントが起こる度にデータマップの更新をすることが必要です。継続的なデータマップの更新は効果的な I.G. を推進する上で非常に重要な要素となります。

4-2．リスクへの対応 - 重複：古いデータの戦略的削除

前述したデータ量の爆発的増加に伴い、企業が抱える重複データや、長年活用されていない古いデータも日々増えていきます。Compliance, Governance and Oversight Council（CGOC）が行った調査[7]では、企業が保有するデータのうち、約 69％はビジネスを行う上では必要がなく、削除を検討出来るという調査結果もあります。データマッピングの結果、識別された重複・古いデータについては積極的に削除していくことが重要です。データを抱えれば抱えるほどリスクも増加するということを念頭に、削除を日々実行していくサイクルを作ることも有効です。組織内のデータがスリム化することで、海外訴訟や当局調査の際求められる eDiscovery 対策にもなり、結果として物理的なサーバや倉庫のスペースの削減、情報漏洩リスクの低減、業務の効率化にも繋がり、コスト削減にも大きく寄与することになります。

また、一方でリティゲーションホールドについても配慮が必要です。リティゲーションホールドとは、訴訟や当局による調査が合理的に予見された時点で、関係者にデータや書類を廃棄せず保持することを通知する証拠保全の行動を意味します。このリティゲーションホールドを実施せず、意図的かどうかに関わらずデータを廃棄してしまったことが判明すると、裁判への妨害行為とみなされ、高額賠償等の懲罰的措置が取られることもあります。

この様に、どのデータを残し、どのデータを削除するのかを慎重に検討し、戦略的にデータの整備をしていくことは I.G. 体制を構築していく上で非常に重要なポイントとなります。

4-3．リスクへの対応：文書管理規定の見直しとアップデート

各産業の法規制や要請に対応した文書・データの保管、廃棄、共有等の規定が策定されているかの確認から始め、各子会社、海外子会社に至るまで実際の規定に沿った運用がなされているかの状況を確認していきます。運用状況を確認する過程で、形骸化している規定、規定が作られていない新しいシステムなどが見つかります。そのそれぞれに対して改善を実施し、同時に最新の法令や規制、各国地域のデータプライバシー規制にまで対応した規定をアップデートすることが求められます。

また、規定の見直し後は、定期的に運用状況をモニタリングし、データの廃棄履歴などの保管状況の監査を実施することも規定が再び形骸化するのを防ぐ意味でも重要なポイントとなります。

[7] Robert F. Smallwood：Information Governance　-Concepts, Strategies and Best Practices. P.6

4-4．リスクへの対応：データ抽出方法の確認

これまで述べてきたようなデータの管理を実施している企業はそれなりに多いかと思いますが、データの抽出までを整理し、把握出来ている企業は少ないはずです。不正調査、国際訴訟、当局調査の現場では、データ抽出を迅速に正確に行うことが求められます。特に日本、米国などの独占禁止法事案でのリニエンシー（課徴金免税制度）では、証拠を提出した順番で課徴金の免除もしくは減免額が決定します。このような例からも、平時からのデータ抽出方法の確認は、非常に重要な点の一つになっています。

具体的には、メール、その他システム毎の抽出方法や形式の確認、抽出にかかる時間のベンチマークを取っておくことが有効です。

4-5．リスクへの対応：データプライバシー規制への対応

EU の GDPR を契機として各国地域で様々なデータプライバシー規制が制定されています。まず、自社が影響を受けるデータプライバシー規制について把握した上で、各規制の要件に合わせた規定の改定、必要に応じてシステムの更新を実施します。また、各規制に違反した際の準備も重要です。GDPR を例に出すと、データ侵害の際の EU 監督機関への 72 時間報告義務が課せられます。また、データ主体からの削除要求などに対応できる体制も求められます。日本国内でも、改正個人情報保護法（2022 年 4 月～ 6 月施行予定）では個人データの漏洩が発生した場合、個人情報保護委員会への報告が義務化されます。

今年 1 月に法律事務所の DLA Piper の発表したレポート[8]によると、GDPR 関連で科された制裁金は総額で 1 億 5850 万ユーロ（約 200 億円）であり、それ以前の 20 カ月に科された制裁金と比べ 40%近くも増えています。この様に、データプライバシー違反による制裁金は今後も増加する傾向にあり、データプライバシー規制に対する体制の構築は企業にとって喫緊の課題だと言えます。

これらのデータプライバシー規制に対する体制を構築するには、プライバシーバイデザイン[9]の概念が参考になります。プライバシーバイデザインとは、プライバシーを取り扱うあらゆる局面で、情報が適切に適法に取り扱われる環境をあらかじめシステムや仕組みに取り入れて構築することを意味します。

また、データプライバシー違反とは何か、違反が発生した場合どう対応するべきか等を事前に検討し、さらに社員に継続的に教育を実施するといった、有事を見据えた体制の構築が求められます。

5. おわりに

昨今度々耳にするサイバーインシデントや、情報漏洩などの有事は、100%全てを回避することは不可能です。何か事が起きた際に適切に素早く行動に移すことが出来る体制を整えておくことは、どの企業にとっても非常に重要な課題だと言えます。また、I.G. はひと時のプロジェクトではなく、継続して取り組むことが非常に大切です。日々データが増大し、テクノロジーの進化、新たな規制や法令が現れるなかで、I.G. も時代や組織の実情に合わせて、細かな調整を日々実施していくサイクルをつくることが重要です。本稿が皆様の Information Governance 検討の一助となれば幸いです。

【参考文献】

[1] Robert F. Smallwood著：Information Governance -Concepts, Strategies and Best Practice-

[2] DAMA日本支部 Metafindコンサルティング株式会社監訳：データマネジメント知識体系ガイド　第二版

8 https://blogs.dlapiper.com/privacymatters/dla-piper-gdpr-fines-and-data-breach-survey-january-2021/

9 https://www.soumu.go.jp/main_content/000196322.pdf