【講演レポート】第96回JIPDECセミナー

DX時代における企業のプライバシーガバナンスガイドブックについて

経済産業省
商務情報政策局 情報経済課　課長補佐　　堂上 和哉氏

IoT・AIといったデジタル技術の革新に比例して、新たなプライバシーリスクが日々発生しており、企業は、データ利活用によるイノベーションの創出とともに、イノベーションから生じうるプライバシーに関わる問題に、真摯に向き合うことが必要となってきています。

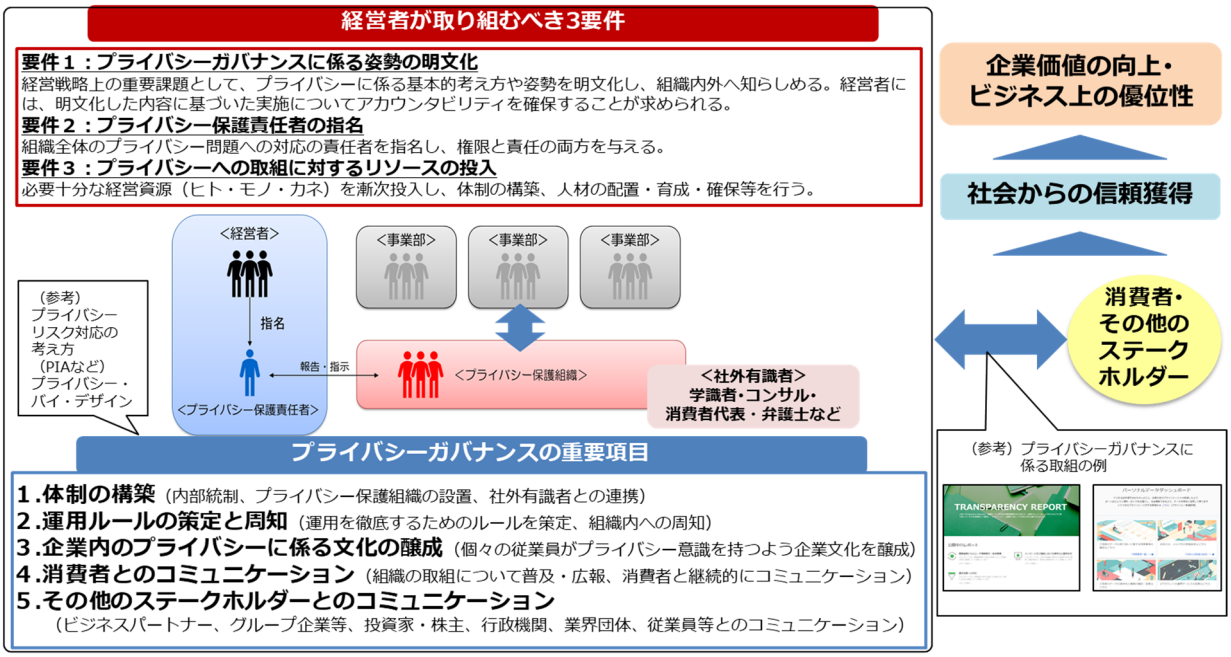
欧米に目を向けると、EUでは基本的人権の観点から、米国では消費者保護の観点から、多額の罰金や制裁金の執行がなされており、経営者がプライバシーに関わる問題を経営上の問題として取り扱うことが認識されています。このような強力な法執行に伴うプライバシーへの対応がある一方で、プライバシーを経営戦略の一環として捉え、プライバシーに関する問題に適切に対応することで、社会的に信頼を得て、企業価値向上につなげている企業も現れてきています。

国内に目を向けると、新たなプライバシーに関わる問題が発生し、人々のプライバシー意識も高まっている中で、必ずしも個人情報保護法などの法令等遵守の範囲にとどまらない形で、企業に対して社会的受容性の観点から疑問が投げかけられたり、社会的批判を避けられないケースも散見されます。プライバシー保護を、単なるコンプライアンス（法令等遵守）として受動的に対応するのでなく、組織全体として能動的に対応し、消費者やステークホルダーへ積極的に取組を説明し、社会からの信頼を獲得していく。そして企業価値向上やビジネス上の優位性につなげていく、という企業戦略が、まさに求められています。

経済産業省・総務省は、2019年10月に「企業のプライバシーガバナンスモデル検討会」を設置し、新たな事業にチャレンジしようとする企業がプライバシーガバナンスの構築のために取り組むべきことを検討し、まさに本日、2020年8月28日に、「DX時代における企業のプライバシーガバナンスガイドブックver1.0」[1]として公表しました。デジタル経済の進展により多くの企業がパーソナルデータを利活用することになると考えます。今回は、特に、消費者のプライバシーへの配慮が必要とされる企業やそのベンダー等の、経営層、管理職、パーソナルデータを利活用する部署に所属する方などを主に想定して、ガイドブックに記載している、プライバシーガバナンスの【構築】と【推進】に関する重要なポイントをご説明します。

[1] 「DX時代における企業のプライバシーガバナンスガイドブックver1.0」
経済産業省プレスリリース：https://www.meti.go.jp/press/2020/08/20200828012/20200828012.html
総務省プレスリリース：
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000098.html

＜図①：「DX時代における企業のプライバシーガバナンスガイドブックver1.0」の概要＞



プライバシーガバナンス構築に向けて、経営者が取り組むべき三要件

企業は、イノベーションの担い手であり、プライバシー保護とデータ活用を単に二項対立として捉えるのではなく、プライバシーに配慮（リスク管理）しながらデータ活用のメリットを最大化（価値創造）していくという視点で捉え、全社的に取り組む必要があります。そのためには、経営者に以下の3点が要件として求められます。

■要件１：プライバシーガバナンスに係る姿勢の明文化

経営者は、プライバシー保護の取組を経営戦略上の重要課題と位置づけ、プライバシーに係る基本的な考え方や姿勢を明文化し、組織内外へ知らしめることが必要です。組織外にも公表することで、組織の信頼を高める根拠にもなります。そして経営者には、明文化した内容に基づいた取組の実施について、アカウンタビリティを確保することが求められます。明文化の取組の具体例としては、宣言の形をとったプライバシーステートメントや、組織全体の行動原則などを策定するケース等があります。

■要件２：プライバシー保護責任者の指名

プライバシーガバナンスの実現には経営者による関与と、上記明文化された内容の具体的実践が不可欠であることから、経営者は「プライバシー保護責任者」を指名し、責任範囲を明確にし、きちんと権限を与える必要があります。経営者はプライバシー保護責任者から報告を求め評価することで、組織の内部統制をより効果的に機能させることができます。

■要件３：プライバシーへの取組に対するリソースの投入

プライバシーへの配慮は事後的に行うものではなく、事前に影響を検討し、戦略、事業、システムへ組み込むことが必要となります。そのため、経営者は、体制の構築、人材の育成・確保・配置等に取り組むことができるように、必要十分な経営資源（ヒト・モノ・カネ）を継続的に投入するという判断が求められます。

プライバシーガバナンスの重要項目

以上ご説明してまいりました、経営者が取り組むべき3要件を踏まえて、ガイドブックでは、企業におけるプライバシーガバナンスを実質的に機能させるために重要な項目を5点、整理しています。

1）体制の構築

【プライバシー保護責任者の役割】

経営者が明文化した姿勢等を実践するため、方針の確立及び体制の構築を進め、当該方針の実施を徹底すること、また、経営者に対し報告を行い、経営者が明文化した内容と合致しているかを絶えず確認する必要があります。

【プライバシー保護組織の役割】

体制を構築するにあたっては、事業の目的達成とプライバシーリスクマネジメントを両立させるために、プライバシー保護責任者の下、中核となる組織（下図②参照）を企業内に設けること。そして、そこに社内情報が集約され、プライバシー問題を発見するために、組織の存在を企業内に周知徹底する必要があります。プライバシー問題は、個人的な感じ方の相違や社会受容性が、コンテキストや時間の経過で移り変わっていくことから、常に関連する情報を収集する必要があります。対象事業の目的を実現しながらプライバシーリスクに対応する、これらをしっかり両立していくための対応策を多角的に検討していく必要がある。そのために他部門と円滑な連携を図っていくことが大切です。

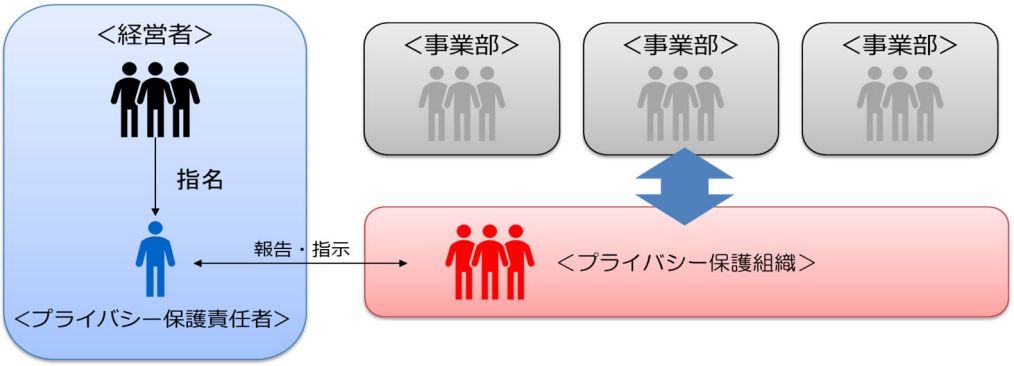
体制を構築することで、問題が発生した場合の情報も、責任者の下へ一本化され、結果、初動対応や経営層・関係者との情報共有・指揮命令が適切になされることにつながります。

なお、体制は企業規模や事業内容によって異なります（下図③参照）。部署の新設が難しい場合でも、兼務の従業員で組織を組成するなど、柔軟に自社のリソースに合わせて実効性のある体制を構築することが重要です。

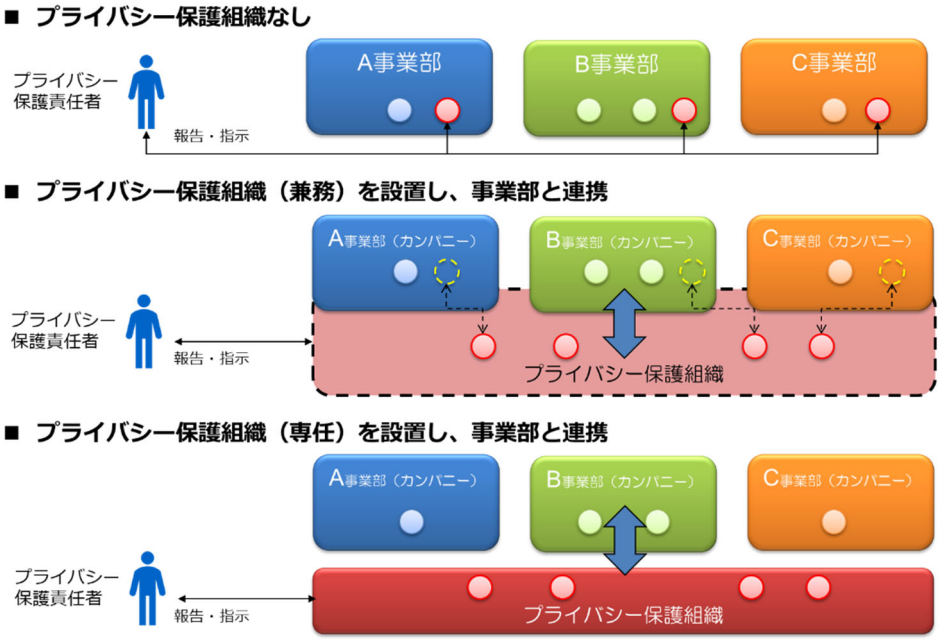
【内部監査部門や第三者的組織の役割】

社内の取組を徹底して、社外からの信頼をさらに高めるためには、内部監査部門による監査など、独立した立場からのモニタリングや評価も重要です。また、第三者的な外部有識者による諮問委員会などによる客観的な意見も聞き入れることができる体制作りが望まれます。

＜図②：体制の構築図＞



＜図③：プライバシー保護組織の企業内での位置づけの例＞



2）運用ルールの策定と周知

社内で体制が実質的に機能するためには、サービスや技術が開発・提供される前に、プライバシー保護責任者やプライバシー保護組織によってプライバシーリスクが把握され適切な検討がなされる必要があります。プライバシー保護責任者の責任の下、プライバシー保護の対策や、どのタイミングで誰がプライバシーリスクを評価するかなどといった観点から、運用ルールを策定し周知徹底することが大切です。ただし、ルールが形骸化しないように、原理・原則の理解や定着を心掛けるとともに、継続してメンテナンスを行う必要があります。

3）企業内のプライバシーに係る文化の醸成

関連部門や担当者に限らず、全従業員が当たり前のようにプライバシーに関する問題意識を持つための啓発活動が不可欠です。例えば定期的な研修教育などと併せて、ジョブローテーションなどの対象にプライバシー保護組織を位置付けるなど、様々な手法で継続的に行うことが有効だと考えます。

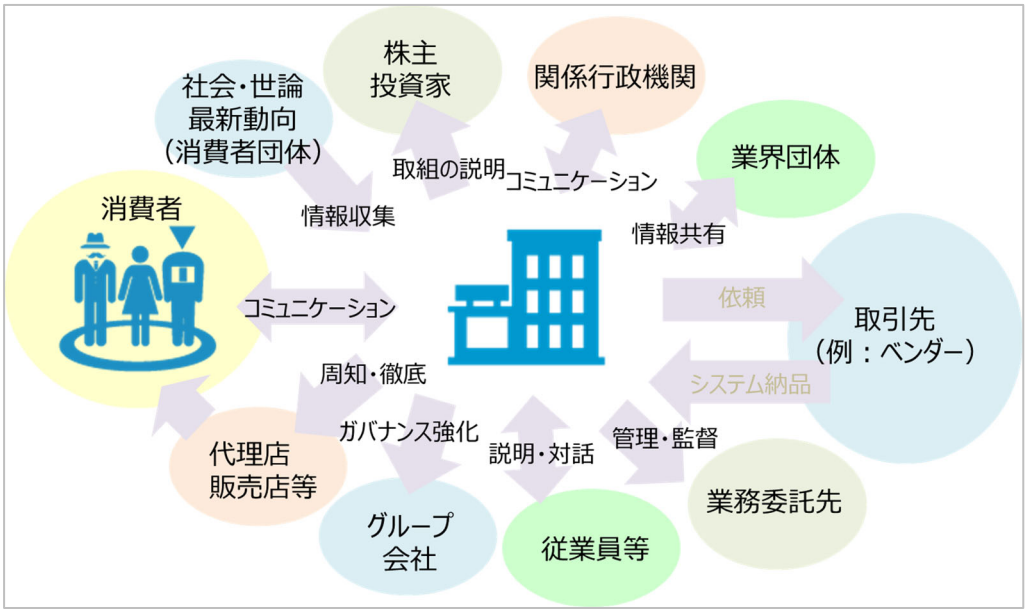
4）消費者とのコミュニケーション

継続的な消費者とのコミュニケーションは必須です。消費者（社会）の受け止め方は刻々と変化しており、法律では許されても道徳的にはNGとみなされ炎上するケースも見受けられます。そういった事象を招かぬためにも、社会の変化を常に把握するとともに、問題発生時に限らず、平時から組織の考え方や新たな取組についても積極的・定期的に発信していくことが重要となっています。

なお、万が一問題が発生した際は、二次被害発生も考慮し専門家の意見も取り入れながら迅速で正確、確実な情報提供を行う必要があります。

5）その他ステークホルダーとのコミュニケーション

その他のステークホルダーとも、消費者と同様に、積極的かつ継続的にコミュニケーションをとることが重要になります。



【ビジネスパートナー（取引先・業務委託先）】

企業が事業を推進する際には、ビジネスパートナーも含めてプライバシー問題に適切に対応しなければ、自社を含む関係企業及び当該事業全体の信頼を失うことになります。

特に、技術革新に比例して新たなプライバシーリスクが発生するため、ベンダーなどシステム関係の取引先と密なコミュニケーションを図り、消費者のプライバシーに対する懸念を絶えず見直すこと、システム面で事前に対応ができないかを検討・対応することが望まれます。

業務を他社に委託する場合、問題が生じたときには委託元にも責任が発生するということを肝に銘じ、適切な対応ができる委託先を選ぶ必要があります。プライバシー問題の発生時には、委託元も顧客や消費者に対して真摯に対応する必要があります。

【グループ企業等】

グループ内の子会社などが主体となって推進する事業であっても、プライバシー問題が発生すればグループ全体のブランドや信頼が失墜しうるため、グループ全体でのプライバシー問題への対応も意識する必要があります。海外に拠点がある場合には、国ごとに対応が必要であることに注意が必要です。

【投資家・株主】

昨今、SDGsへの関心も非常に高まっている中で、投資家・株主も企業業績への影響や社会的責任という観点から、リスク管理体制の強化についても、コストではなく先行投資として評価する傾向がみられます。そのため、株主や投資家に対しても、企業のプライバシー問題への対応を明確に説明することがますます求められてきています。

【関係行政機関】

個人情報保護委員会等も、パーソナルデータの利活用やプライバシー問題に取り組む行政機関の相談窓口を設けているので、プライバシーリスクが高いと思われる事業を開始する際には、行政機関に事前に相談を行うことも重要となります。

【業界団体】

同業他社が同じ技術分野でプライバシー問題を起こしてしまうと、自社の同様のサービスにおいても消費者の信頼を失ってしまう可能性もあるため、業界全体で取り組んでいるケースもあります。業界団体を通じて積極的に情報提供・入手を行うとともに、入手した情報を有効活用できるような環境を整備することも必要となります。

【従業員等】

企業は従業員のプライバシーに関する情報を取り扱うことが多く、従業員へのプライバシーにも配慮が必要です。他方で、事業運営上の要請から従業員のプライバシーを制限する必要が生じる場面や、従業員に関する情報の漏えいのリスクも存在します。このため、従業員もコミュニケーションをとるべき主体として捉え、対話や従業員代表を通じた説明・周知などの取組が重要となります。さらに、自社の従業員だけでなく、求職者や退職者、取引先の従業員に対しても配慮が必要であるということをしっかり認識しておく必要があります。

なお、ガイドブックでは、最後に参考として、プライバシーリスクをどのように精査すべきかその手法についても記載しています。ぜひ、ガイドブックの本体を参照いただきたいと思います。例えば、パーソナルデータの特定とライフサイクル整理、プライバシーリスクの特定の際に参照いただけるような発生しうるプライバシー問題の例、リスク分析・評価・対応検討を行う手法であるプライバシー影響評価（PIA）（今後JIS規格発行予定）等についても、紹介しています。

最後に

今回、本日ご説明のような形でガイドブックを取りまとめましたが、今後はこちらの内容の普及に努めるとともに、「プライバシー」の考え方がこれからどんどん変わっていくということを我々も肝に銘じ、必要なアップデートを随時行きたいと考えています。今回ガイドブックに「Ver.1.0」と明記したのは、そのような思いからです。

個人的には、日本全体でプライバシーガバナンスの考え方を広げていくためには、企業活動の連鎖が不可欠であり、企業の皆様のプライバシー問題に対する姿勢や実現に向けた取組を積極的に公表していただき、それを企業間で参照しあっていくことは重要だろうと考えています。これが大きなムーブメントになれば、日本の「プライバシー問題」に対する対応が、全体として進んでいくのではないかと考えています。そのために政府として何ができるかも、考えていきたいと思います。

経済産業省　商務情報政策局 情報経済課　課長補佐　　堂上 和哉氏
2014年京都大学法学部卒業、経済産業省入省
原子力立地・核燃料サイクル産業課、石油・天然ガス課、大臣官房総務課を経て、現職
データ利活用の促進、クラウドの安全性評価制度の運用、プライバシー保護やデジタル時代のガバナンスの在り方の検討等を担当

本内容は、2020年8月28日に開催された第96回JIPDECセミナー「DX企業のプライバシーガバナンスガイドブックver1.0（案）」講演内容を取りまとめたものです。