プライバシーガバナンス構築に向けた具体的な取り組みの進め方

–パーソナルデータの持続的な活用に向けて–

株式会社 野村総合研究所
CX コンサルティング部
チーフコンサルタント　南島　安平

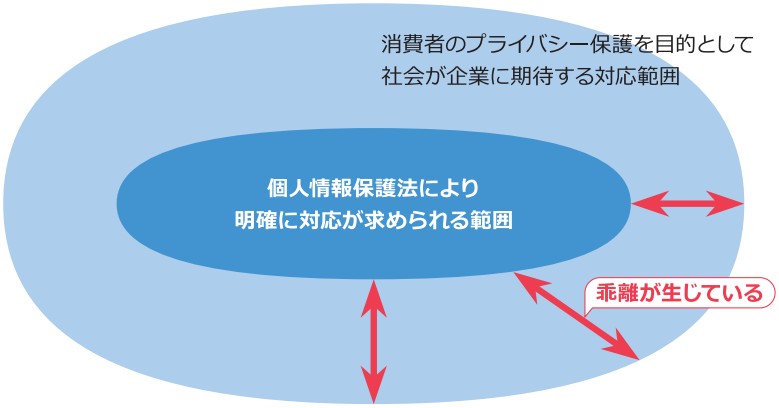
1　はじめに ―企業による自主的なプライバシー保護対応の必要性―

2022 年 4 月に「令和 2 年改正個人情報保護法」が施行され、対応を迫られた企業も多いと思うが、近年、消費者のプライバシー保護を目的として社会が企業に期待する対応範囲が広がりつつある。これまで多くの企業にとって消費者のプライバシー保護対応とはすなわち法令順守を意味していた。しかしながら、近年、情報技術の進展やビジネスモデルの変化に対して、法改正がタイムリーに追いつけていない状況が発生している。その結果、法令が明確に求める対応範囲と社会が企業に期待する対応範囲との間に乖離（かいり）が生じ、企業によるプライバシー侵害（いわゆる炎上事件）をきっかけに乖離が顕在化しつつある。

企業が社会からの期待に応えられず事業活動を大きく転換せざるを得なかった事例として、LINE 社によるユーザーデータの海外保管・アクセス停止や、ヤフー社における Yahoo! スコア事業の廃止が挙げられる。いずれも個人情報保護法に違反していたわけではないが、消費者のプライバシー保護対応が不足しているとして社会的に大きく問題視され、事業方針の変更を迫られた。

乖離の状況はその企業が取り扱うデータの量や性質によって異なるが、今日、安定的かつ持続的なパーソナルデータ活用の高度化を進めるためには、法令対応を超えて自社のビジネスモデルに合わせた自主的なプライバシー保護の取り組み、すなわち「プライバシーガバナンスの構築」が企業には求められている。

図表 1　プライバシー保護の観点から企業が考慮すべき範囲



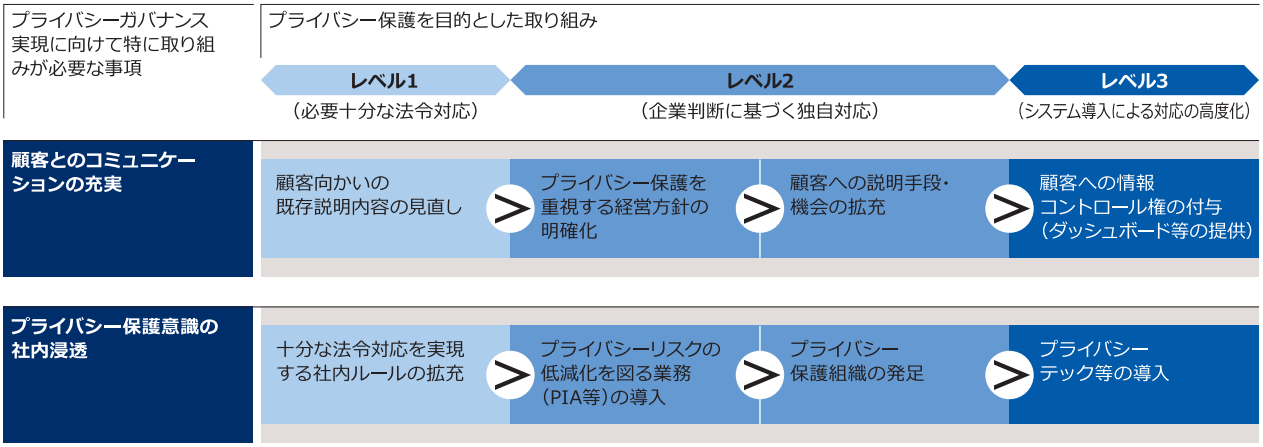
出所）NRI 作成

図表２　プライバシーガバナンスの重点項目

1	体制の構築（内部統制、プライバシー保護組織の設置、社外有識者との連携）
2	運用ルールの策定と周知（運用を徹底するためのルールを策定、組織内への周知）
3	企業内のプライバシーに係る文化の醸成（個々の従業員がプライバシー意識を持つよう企業文化を醸成）
4	消費者とのコミュニケーション（組織の取り組みについて普及・広報、消費者と継続的にコミュニケーション）
5	その他のステークホルダーとのコミュニケーション（ビジネスパートナー、グループ企業等、投資家・株主、行政機関、業界団体、従業員等とのコミュニケーション）

注）青色の網掛けは多くの企業において特に重要であると筆者が考える部分
出所）総務省・経済産業省「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 ver1.2」より NRI 作成

図表３　プライバシーガバナンス構築に向けた段階的な取り組み



出所）NRI 作成

2　プライバシーガバナンス構築にあたっての重点項目

自主的なプライバシー保護対応とは何をどのように進めることを意味するのか。参考にすべき情報として、政府はプライバシーガバナンス構築に向けた重点項目を五つ挙げている（図表２）。

個人情報保護法を順守することで、重点項目１～５のそれぞれについて抜け漏れなく対応を図ることができるが、筆者はこれまでのクライアント企業とのディスカッションを通じて、炎上事件を避けるために最も効果的な「顧客とのコミュニケーションの充実（重点項目４に関連）」と、より実効性のある「プライバシー保護意識の社内浸透（重点項目３に関連）」について、多くの企業においてさらなる取り組み余地があると考えている。

コミュニケーションの充実とプライバシー保護意識の社内浸透をどう図るか。先行してガバナンス構築を進める企業の状況を踏まえると、データ活用の高度化やプライバシー保護業務の広がりを踏まえた段階を追った取り組みが重要であることが見えてきた。

本稿では、上記二つの課題に焦点を当て、プライバシーガバナンス構築に向けた取り組みを「レベル１　必要十分な法令対応」「レベル２　企業判断に基づく独自対応」「レベル３　システム導入による対応の高度化」の３段階に分けて整理する。

図表４　企業において顧客に個人情報の取り扱い方を通知する文書

	文書の種類	通知内容	設置根拠
1企業につき一つ存在	プライバシーポリシー	● 個人情報保護を推進する上での考え方や方針を示す文書	● 個人情報の保護に関する基本方針６（１）※設置が望ましいとされている
	コーポレートとしての通知	● 企業として保有している全ての個人データに関する取り扱いの状況を示す文書	● 個人情報保護法第32条（保有個人データに関する事項の公表等）
企業内に複数存在する場合もある	サービスごとの通知	● 個人情報を取得する際に、通知する文書	● 個人情報保護法第21条（利用目的の通知または公表）

出所）NRI 作成

3　顧客とのコミュニケーションの充実に向けた取り組み

ここでのコミュニケーションとは、企業によるパーソナルデータの取り扱い状況の説明や顧客自身が企業に提供するデータ項目・提供先を管理する機会（いわゆるダッシュボード）の付与を意味する。顧客が抱く企業による情報利用に対する抵抗感や情報リテラシーの有無を考慮して、複数のコミュニケーション手段を提供することで、画一的な法令対応では培うことができない顧客の企業に対する信用醸成に寄与する。

1）顧客向かいの既存説明内容の見直し（レベル１の取り組み）

企業において個人情報の取り扱いについて顧客に通知する文書（規約・ポリシー等）は複数存在する。文書の種類、通知内容および設置根拠を図表４に示す。

このうち「サービスごとの通知」は文字通り個別のサービスにおいて作成される文書だが、多くの企業において記載形式（文書の名称・構成・表現等）が統一されておらず、同一企業が提供するサービスであるにもかかわらず、あるサービスでは「プライバシーポリシー」という形で、また別のサービスでは利用規約に含まれる一つの条項として通知されている。

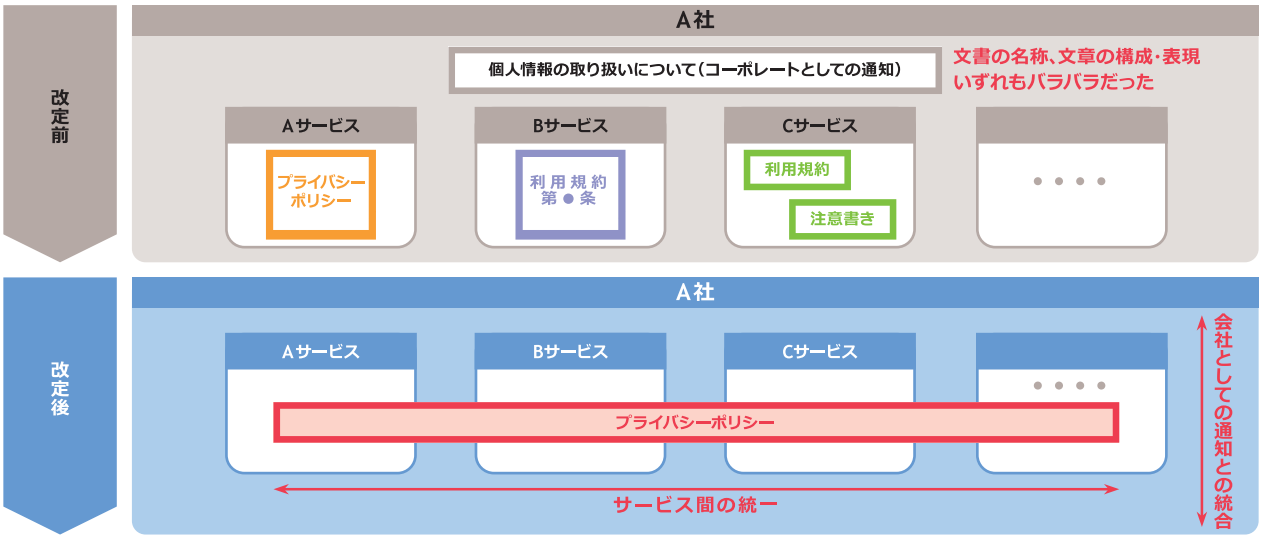
こうしたバラバラな通知状況は、サービス横断的なデータ活用を企画する際にしばしば懸念をもたらす。企画している活用方法が対象サービスの通知文書全てにおいて、適切な説明（場合によっては同意取得）を行えているかどうか、記載形式が異なり判断しづらいためである。

この懸念を払拭（ふっしょく）するため、個人情報の取り扱いについて顧客に通知する文書（規約・ポリシー）をより実態に即した形、より顧客が理解しやすい形へと改定する動きが出ている。改定にあたっては、サービス間や企業全体としての通知文書（プライバシーポリシーやコーポレートとしての通知）との平仄（ひょうそく）を意識し、企業として顧客のプライバシー保護に取り組む姿勢を統一、明確化することが求められる。

2）顧客への説明手段・機会の拡充、顧客への情報コントロール権の付与（レベル２～３の取り組み）

企業による自主的なプライバシー保護対応として

図表 5　通知文書改定の取り組み



出所）NRI 作成

図表 6　通知文書とは別に整備するわかりやすいユーザーガイドの例

NTTドコモ: パーソナルデータについて

Yahoo！JAPAN: プライバシーセンター

出所）株式会社 NTT ドコモ「知ってナットク！ドコモのパーソナルデータ活用」
https://www.docomo.ne.jp/utility/personal_data/（2022.7.1 時点）
ヤフー株式会社「プライバシーセンター」https://privacy.yahoo.co.jp/

二つ紹介する。一つは法定で整備が求められる通知文書を補完する目的で、データ処理方法等について、ウェブサイトやプレスリリース等で説明するというものである。

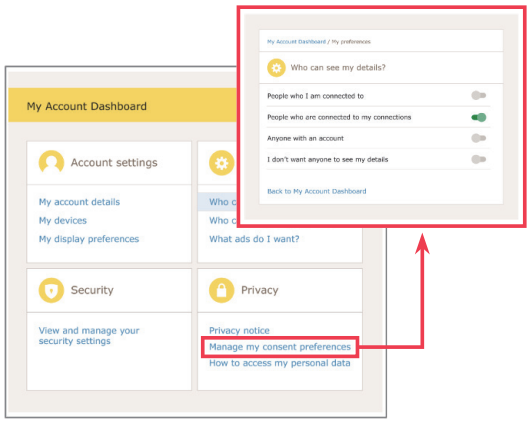
データ活用の高度化が進む企業においては、通知文書とは別にイラスト等を用いたわかりやすいユーザーガイドを提供しているところもある。こうしたガイダンスは、長文になりがちな通知文書を倦厭（けんえん）する（しかし、自身の情報の取り扱い方は気になる）顧客や、自分の知りたい内容だけをピンポイントで確認したい顧客にとって有用な情報提供手段となる。

もう一つは、より高度なコミュニケーション手段の提供として、第三者提供先や利用目的について顧

図表 7　企業が収集している情報を顧客自身が管理する仕組み（ダッシュボード）の例

英国当局（ICO）が推奨するダッシュボードの例

● アカウント設定の同意状況管理ボタンから、情報の開示範囲を設定する画面へと遷移する



NTTドコモによる実装例

● データの提供先（第三者提供先）について顧客自身が選択・設定することができる

出所）ICO ウェブサイト https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/
株式会社 NTT ドコモ「パーソナルデータダッシュボード」https://datadashboard.front.smt.docomo.ne.jp/（2022.7.1 時点）

客が自身の同意状況を管理する仕組み（いわゆるダッシュボード）を導入することである。スマートフォンのオペレーションソフトでは既にユーザー自身が情報を管理する機能が提供されているが、顧客のライフステージやスタイルに合わせてさまざまなサービスを展開する企業グループにおいては、同様の機能の提供が望まれる。英国のデータ保護当局であるICO（Information Commissioner's Office）はダッシュボードの提供を推奨しており、国内でも一部の事業者において既に導入されている。

株式会社 NTT ドコモが導入している「パーソナルデータダッシュボード」では、データ項目ごとに、提供範囲をユーザー自身が設定することができる。パーソナルデータの提供に一度同意した後も、意向に応じて同意の撤回を可能にするダッシュボードの機能は、企業によるフェアなデータ活用を裏付けるものとして、消費者の信用に資すると考える。

4　プライバシー保護意識の社内浸透に向けた取り組み

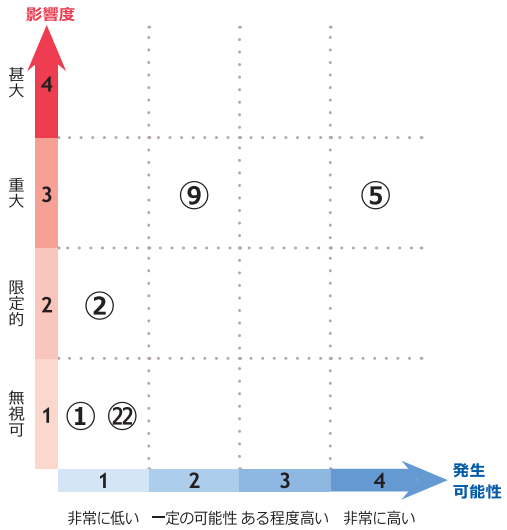
コミュニケーション手段を多様化し、顧客からの信用を醸成する一方で、併せて組織の体制を充実させていく必要がある。データ活用の担当者が曖昧な認識のままデータを取り扱うことがないように、プライバシー保護意識の社内浸透も段階的に高度化していくことが求められる。

1）プライバシーリスクの低減化を図る業務の導入（レベル２の取り組み）

多くの企業の社内規定において、「個人情報に該当する場合は○○せねばならない」といった形の規定が確認できる。こうした一律の対応はデータ活用の自由度を無用に制限したり、表面的な対応による思わぬ事故を招いたりする恐れがある。

パーソナルデータを活用する際、データの機微性や取り扱い量に応じて想定されるリスクは異なる。このプライバシーリスクを可視化し、リスクに応じた保護措置を講じる取り組みとしてプライバシー影

図表 8　リスクマッピング（左）と評価基準（右）の例



(影響度)レベル		基準
4	甚大	●利用者に回復不可能な多大な不利益が生じ、これに伴い、企業の信用失墜や経済的損失が生じる(心理的・身体的疾患、口座番号、暗証番号の流出等)
3	重大	●利用者に一定の不利益が生じるものの、回復可能であり、企業の信用等への影響はそれほど大きくない(迷惑メールの受信、アカウントの乗っ取り等)
2	限定的	●一部の利用者に不安感を与え、企業の信頼等に影響が及ぶ可能性があるが、その範囲は限定的(サービスへのアクセス拒否、利用方法に関する説明不足等)
1	無視可	●利用者への不利益の程度は極めて小さく、企業への影響は無視できるレベル(同意取得時にアプリケーション上にチェックを入れる煩わしさ等)

(発生可能性)頻度		基準
4	非常に高い	●安全管理等に不備があるため、リスク発生が容易に想定される(セキュリティー対策の不備で情報漏えい等が発生する等)
3	ある程度高い	●安全管理の一部に不備があるため、リスク発生の可能性がある(ノートPCや携帯電話などのモバイルの紛失等)
2	一定の可能性	●安全管理措置により、リスク発生の可能性は低い(注意喚起のメッセージが表示される中でのメール誤送信等)
1	非常に低い	●リスク発生の可能性は極めて低い(入館証読み取り機でセキュリティー対応の取られた室内の書類の紛失等)

出所）個人情報保護委員会「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―（概要）」より NRI 作成

響評価（PIA：Privacy Impact Assessment）が挙げられる。

PIA ではデータ活用施策ごとに取り扱いの影響度とインシデント発生の可能性の 2 軸で評価を行う。評価の結果はマッピングされ、マップの右上に位置する施策についてはそのまま続行とはならず、プライバシーリスクを低減化する措置の再考が求められる。

PIA を導入することで、「個人情報＝○○せねばならない」の一律の対応から離れ、データ活用の担当者自身がプライバシーリスクを意識することにつながる。

2）プライバシー保護組織の発足（レベル 2 の取り組み）

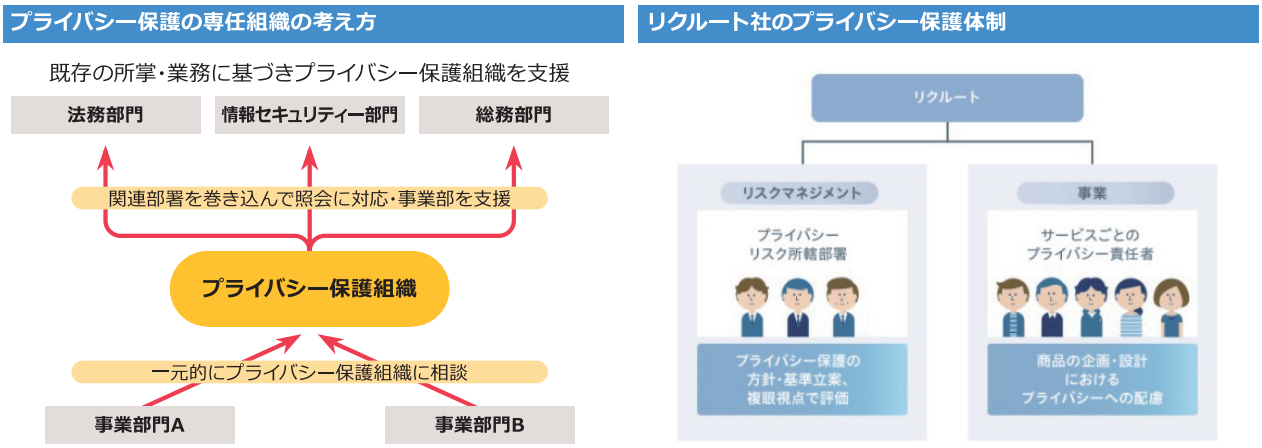
PIA をはじめとするプライバシー保護業務が確立してくると、専任組織の設立や事業部門側でのプライバシー保護担当者の配置が有用となる。プライバシーリスクの低減化にあたっては、法務、情報セキュリティー、顧客満足度向上等、複数の切り口から取り組むことが想定されるが、事業部門側が課題の所在を自ら切り分けて関係組織に個別に相談することは難しい。場合によっては、相談してもたらい回しになるといったことも想定される。

そこで、事業部門からの相談を一元的に受け付ける窓口がプライバシー保護組織である。保護組織は相談内容に応じて関係部署と協働しながら事業部門を支援する。また、リクルート社のように、事業部門側にプライバシー保護担当者を設置することで、プライバシー保護組織に対する事業部門側の窓口を明確にし、より組織間の緊密な連携を可能にしている企業も見られる。

3）プライバシーテック等の導入（レベル 3 の取り組み）

個人情報＝○○といった画一的な対応から離れ、プライバシーリスクを可視化し、リスクに見合った対応をその都度検討する業務が増加、定常化してくると、より効率的に業務を遂行する仕組みづくりが求められる。近年、プライバシー保護業務をサポートするツールとしてプライバシーテックと呼称される製品群が登場してきた。プライバシーテックは企

図表 9　プライバシー保護の専任組織の考え方（左）とリクルート社の事例（右）



出所）NRI 作成
株式会社リクルートウェブサイト https://www.recruit.co.jp/privacy/governance/

業内におけるデータの取り扱い状況を一覧化するデータマッピング機能やユーザーからの同意取得状況を統合的に管理する機能などを有し、企業におけるプライバシー保護業務を包括的に支援する。

ただし、あくまでテクノロジーは業務をサポートするものである。前述の PIA 等を通じたプライバシー保護意識の社内浸透が十分図られない中でプライバシーテックを導入しても、機能を十分使いこなすことができず、効果が限定的になる。製品導入ありきの検討ではなく、まずは PIA 等のプライバシー業務を手作業でも運用してみることをお勧めしたい。

5　おわりに

本稿では企業による自主的なプライバシー保護対応として、「顧客とのコミュニケーションの充実」と「プライバシー保護意識の社内浸透」の観点から段階的な取り組みが重要であることを紹介した。

ユーザーガイドやダッシュボードの提供は総務省が示す「電気通信事業における個人情報保護に関するガイドライン」において推奨されており、また、PIA の実施手順は個人情報保護委員会が案内を行っている。本稿で紹介した取り組みの一部が将来的な法改正により義務化される可能性もあるが、より本質的には企業自らがプライバシーリスクの存在を認識し、安定的かつ持続的なパーソナルデータ活用の高度化を進める上で必要なガバナンス構築に取り組むことが重要と考える。

●…… 筆者
南島　安平（みなみしま　やすへい）
株式会社野村総合研究所
CX コンサルティング部
チーフコンサルタント
専門は、データ活用の高度化を軸とした事業戦略立案、データガバナンス
E-mail: y-minamishima@nri.co.jp