データ保護・プライバシー規制強化の潮流

～顧客との信頼関係を確保するための取組み

松岡　靖典

2019年入社
金融サービス本部
ファイナンス&リスクサービス
プリンシパル・ディレクター
（所属名 2020年2月時点）

GDPR（EU一般データ保護規則）の施行から2年弱が経過。デジタル経済の著しい発展を背景に、グローバルベースでデータ保護・プライバシー規制強化の波が押し寄せている。

重要な点は、顧客個人が事業者の保有するデータへ関与する権利が強化されたこと。金融機関の立場からみると、個人データという「重要な資産」に対して、従来同様に外部流出・漏洩がないように「適切に管理・保護すること」はもちろん、「重要な資産の管理状況を説明できること」や「重要な資産の利用方法を指定できるようにすること」が求められる。

このプライバシー規制に対応するため、金融機関は、従来の「データ保護」を中心とした取組みを発展させ、全社包括的なフレームワークを構築する必要がある。

データ保護・プライバシー規制は黎明期から成長期にあり、強化の流れは変わらない一方、各地域・国が異なる内容・スピードで規制を行うだろう。このような状況下、金融機関は、自らのビジネスを踏まえたリスクプロファイルや既存の統制手法などを考慮し、取組みのアプローチを検討すべきと考える。

押し寄せる規制強化の波

グローバルベースでデータ保護・プライバシー規制強化の動きが強くなっている。ポイントは、顧客個人に対して自身のデータに対するアクセス権を強化していることにある。ビジネス上のデータ利活用の発展につれ個人データの価値が大きく増加したことに伴い、個人データの適切な利用確保のため、「個人に対してデータの利用状況を知る権利や利活用の判断できる権利を確保」する枠組みが必要となったのである。

幅・深度・スピードが異なる規制

各地域・国当局のデータ保護・プライバシー規制は、内容や進捗にばらつきがみられる。日米欧等主要な地域での足元の規制内容・状況は次の通り（図表1）。

欧州～制裁本格化とeプライシー規制の動き

GDPRは、データ保護・プライバシー規制強化の先駆けであり、「忘れられる権利（削除権）」「データポータビリティの権利」「プロファイリングを拒否する権利」を規定している。足元では制裁が本格化している。ブリティッシュエアウェイズ（約250億円）を含め、昨年以降で約170件/約540億円の制裁が課された（2020年2月現在）。グーグルへの制裁（約62億円）は情報漏洩ではなく不適切な説明・同意取得プロセスが原因であり欧州当局の本気度がうかがえる。また、クッキー情報の取り扱いを規定しているeプライバシー「指令」を「規則」に格上げすることが検討されている。

米国～CCPAの施行

本年1月にCCPA(カルフォルニア消費者プライバシー法)が施行された。一定要件に該当する事業者に対して州民の情報の保護を課している。州民に対して、「収集データの運用方法の開示請求権」「具体的な収集データを取得する権利」「収集データ削除の要求の権利」「個人データの売却停止の権利」を認めている。

日本～個人情報保護法の改正

本年に個人情報保護法改正の法案審議の予定である。主な内容は「個人データに関する個人の権利」、「事業者の責務」、「データ利活用の施策」、「法の域外適用、国際的制度の調和」等。特に、個人データでは本人の関与する権利が強化され、個人データの利用予定・消去の請求、第三者移転の停止請求の緩和や、電子データでの開示請求の拡大が図られる方向である。また、クッキー情報は法規制上の取り扱いの整理・明確化がなされる見込みである。

その他の国々～GDPRへの追随等

インド、ブラジル、タイ等でGDPRをモデルにした規制を検討中。また、中国やロシア等の社会主義国ではデータローカライゼーション（データサーバーの国内設置）規制が課されている。

図表1 日米欧でのプライバシー規制の状況

	規制	主な内容	足元の動き等
欧州	GDPR（EU一般データ保護規則） 【2018年5月施行】	• **データ主体の権利** ①忘れられる権利（削除権）② データポータビリティの権利 ③ プロファイリングを拒否する権利 ④ 収集目的等の情報提供を受ける権利 • **事業者の責務** ① 取り扱いルールの整備 ② データ取り扱いのための管理態勢 ③ データ移転のルール整備 • **制裁** 最大20百万ユーロ もしくは売上高の4%の高い方	• 制裁が本格化。巨額の制裁金も含め、2019年1月以降約140件/約511億円（2020年1月現在）。 • eプライバシー規則（いわゆるクッキー法）制定への動きあり。通信データ上のプライバシー保護強化が見込まれる。
米国	CCPA(カルフォルニア消費プライバシー法) ～カルフォルニア州民の情報が対象 【2020年1月施行】	• **データ主体の権利** ①収集データの運用方法を開示請求する権利 ②具体的な収集データを取得する権利 ③データの削除を要求する権利 ④第三者へのデータ売却停止を要求する権利 • **事業者の責務** プライバシーポリシーの制定と年次見直し • **制裁** 違反1件あたり最大2500ドル（故意の場合最大7500ドル）	• **2018年6月に州議会での法案通過後、種々の改正作業を経て2018年10月に州知事が承認。** • **罰則規定の執行は2020年7月目途の見込み。**
日本	個人情報保護法の改正大綱 【2020年改正法案審議の見込み】	• **データ主体の権利** ①個人データの利用停止、消去、第三者提供停止請求の要件緩和 ②開示請求の充実（電子データでの開示等）③開示対象データの範囲拡大、④個人データの第三者提供の規制強化 • **事業者の責務** 漏えい等報告・本人通知の義務化 • **データ利活用の施策** 「仮名化情報」の創設 • **制裁** 課徴金の見直しは継続検討	• **2019年12月に制度改正大綱がとりまとめられ法案化作業の過程。** • **個人データに対する本人の関与を強化。データの利用停止、消去請求、第三者提供停止の権利を拡大。** • **クッキー情報に関し、個人データとの関係を整理し、規制対象として明確化される見込み。**

出所：公開資料よりアクセンチュアまとめ

プライバシー規制対応のフレームワーク

金融機関は、従来より、個人データの「保護」の観点から、外部不正アクセス等によるデータ流出を防止すべくシステム対応を中心に取り組んでいる。プライバシー規制では、顧客が自身のデータへのアクセス権を保有するため、さらに管理を発展させ全社包括的なフレームワークが必要となる。そのフレームワークの基本的な要素は、①プライバシープログラムガバナンス、②プライバシーデータの検知・分類、③顧客要求に沿ったプロセスデザイン、④テクノロジー、⑤トレーニングである（図表2）。

プライバシープログラムガバナンス

ガバナンス態勢のポイントは、a組織上の管理体制、bルール、cモニタリングとなる。組織上の管理体制では、DPO（データプロテクションオフィサー）やCPO（チーフプライバシーオフィサー）の責任者を設置し、リスク検知や組織横断的な改善対応の権限を与える。ルールでは、全社レベルでの基本方針、手続・手順まで一連の規定を明確に定める。モニタリングでは、不適切な運用の有無を定期的にモニタリングするとともに、発生した問題に対する改善対応が計画通り進捗しているかを確認する。既にGDPR施行のための枠組みは整備済の金融機関も多数あるが、あらためてプライバシー規制の観点からのルールの見直し、そのルール変更に基づくモニタリング内容の変更が必要となる。

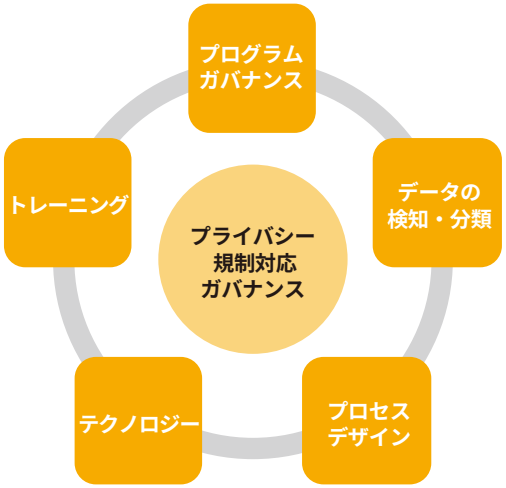
プライバシーデータの検知と分類

顧客のデータへのアクセス権に応えるためには、金融機関は個人データを適切に分類、保存、検知できる状態にしなければならない。現状、金融機関が預かる個人データは、各種のデータベースに分散され、必ずしも統合されていない。まずは、法規制の対象となる個人データが、どこに、どのような種類が、どのように保存されているかを把握する必要がある。また、個人データには、文書等の非定型データも多く含まれ、データ検知は困難な状態にある。しかしながら、プライバシー規制の対象がデータの種別は問わない以上、非定型データも含めたデータに対する検知・分類のツールが必要となる。すべてのデータを検知・分類することを可能とするデータプラットフォームや検知ツールを一朝一夕に導入することは困難であり、リスクベースで優先順位を付けた取組みとなるかもしれないが、あくまでも対象はすべて個人データである。

顧客要求に沿ったプロセスデザイン

プライバシー規制では、個人に対して、a個人データの利用方法の開示、b個人データ利用可否の判断、c個人データの削除の権利等を認めている。したがって、個人データが関連する業務プロセスは、データを取得する局面、取得するデータ等を明確にし、これらの個人の権

図表2 プライバシー規制対応プログラムの5要素



出所：アクセンチュア方法論

図表3 高まるプライバシーや消費者権利の規制に対するアプローチ

戦術的 → 戦略的

	規制対象のデータ主体のみを統制	規制に合わせ既存データプライバシーモデルを強化し統制	より広い「消費者権利」に基づく態勢により統制
長所	• 限定的なスコープ、ROI上の透明性高い • 規制の文言や精神を忠実に遵守することが可能	• 既存のエンタープライズ機能を再利用する機会（NYDFS、GDPR対応） • 機能の開発と配置の複雑さを軽減	• 「一度の構築による多くの問題解決」アプローチにて効率性高い • 規制に先駆けて機能開発することが可能
短所	• 追加の規制が発動した場合に効率性低下 • 標準化されておらず、平仄のない「パッチワーク」の可能性	• 法規制の変更に際して継続的にモデル見直しの可能性 • 法規制の対象外の統制に対する反発の可能性	• 対象となる規制の「最大公約数」を定義する困難さ • 全社的な協力・連携を構築することに時間を要する可能性

出所：アクセンチュア方法論

利が実現できるように設計されなければならない。また、業務プロセスにはサードパーティーが関与していることが多い。サードパーティーのリスク管理・統制、その成熟度は、金融機関の基準に合致していないことがある。業務プロセスの統制強化では各サードパーティーを含めた取組みが必要となる。

テクノロジー

法規制対応の重要課題は、データ削除ができない、個人データの匿名化ができない、その他当局要請をクリアできないシステム等を特定し改善することである。このようなシステムへの対応は、場合によっては短期間で多大のマニュアル作業を要する可能性がある。効率的・短期間の改善対応にはテクノロジーを駆使する必要がある。

トレーニング

プライバシー規制の枠組み（体制）を構築しても、従業員の意識向上が図れなければ、形骸化し真の目的は達成できない。結果、テクノロジーに多大な投資をしても、不正・不適切な運用により多額の罰金に結び付きかねない。研修により従業員の徹底的な意識向上を図る必要がある。研修は2つのレベルがある。1つは意識向上を目的とした全社レベル、もう1つは顧客接点のある一線のスタッフに対して担当業務・役割に合わせた、より具体的な運用に関する研修である。

規制対応へのアプローチタイプ

データ保護、プライバシー規制強化の潮流は変わらず規制の範囲を拡大し、同時に、各地域・国の当局が異なる内容の規制を制定するだろう。このような状況のもと、金融機関がプライバシー規制に対応するアプローチは、「戦術的：現在の法規制だけに対応」から「戦略的：今後の規制強化や各地域・国の規制を視野に入れた態勢と幅がある。米国金融機関の例では主に3種類のアプローチがある。①規制対象のデータ主体のみを統制、②規制に合わせ既存データプライバシーモデルを強化し統制、③より広い「消費者権利」に基づく態勢による統制である。いずれも長所・短所がある。金融機関は、自らのリスクプロファイルや既存の個人データ統制手法を考慮し、検討する必要がある（図表3）。

おわりに

プライバシー規制は黎明期から成長期に移行しつつあり、当面、金融機関にとっての負荷が高い取組みとなる（特にグローバルベースでビジネスを行う金融機関の負荷は高い）。一方、別の見方をすれば、単なる法規制遵守やデータセキュリティの枠を超え、リスク管理部門、システム部門、事業部門が一体となり全社的にプロアクティブなアプローチをとることにより、金融機関は顧客との信頼関係を強固にすることが可能となるだろう。