ISSUE 120

# BOARD PERSPECTIVES:

取締役会のリスク監視：Risk Oversight

## 責任ある個人情報保護：取締役会はその役割を果たしていますか

**個人情報保護に関する問題について役員室で多くのことが話し合われており一部の取締役はこの話題に疲れを感じています。それでも、各取締役会は急速に進化するこの分野と、それが会社のビジネスモデルに与える影響に注意を払う必要があります。**

プロティビティは、2019年6月の全米取締役協会（NACD）のイベントでのディナーラウンドテーブルにおいて、現役取締役のグループと会い、この分野での経験について話し合いました。以下はその議論の中で取り上げられた重要なポイントの一部です。

**個人情報保護プログラムが強調されていることを認識する：** 個人データ保護のコンプライアンスプログラムの厳格なテストと、企業が準拠する複雑な法的マトリックスを作成することが変化の推進力となっています。個人情報に関する規制の強化、新しい技術の進化、個人データの使用に対する消費者の監視、ベンダーネットワークの成長、そしてグローバル化とローカリゼーションの力などがその要素です。この推進力は、現在の組織にとっての個人情報保護の意味を再定義し、企業の責任に焦点を当てたものとなっています。これらは取締役会が適切な監視を行わなかったと主張する集団訴訟を生み出しており、企業が公開する報告書には適切な個人情報保護とセキュリティ管理が実施されていると報告されているが実際にはそうではないことを明らかにしました。

**重要なポイント —** 取締役と経営陣は個人情報とセキュリティ環境の複雑さを認識し、会社のビジネスモデルへの影響を判断する必要があります。CIO、顧問弁護士、コンプライアンス担当役員、事業ユニットの責任者などのビジネスリーダーや運用グループが最新の規制に対応できるように、取締役会が調整と支援を促進する必要があります。

**正しい質問をする：** 個人データ保護の観点から、何が合法的かだけでなく倫理的で会社のブランドと整合しているものを理解することに取締役会は取り組んでいます。現在の個人情報保護法の条文に準拠することがひとつの基準です。個人データ保護が組織の企業戦略とビジネスモデルにどれくらい不可欠かを理解することと、経営陣が消費者データの適切な使用をどのように定義しているかを理解することとは、別々の問題であり、より高い基準です。ラウンドテーブルの参加取締役は、経営陣がこれらの問題をどのように定義したかを問い、理解し、その過程でデータ収集と管理に関する望ましいリスクプロファイルと要求項目、そして関連する責任を明確にすることが取締役会の主な役割であるという点で合意しました。

protiviti®

*Face the Future with Confidence*

**重要なポイント —** 取締役が正しい（そして難しい）質問をしなければならないという古い決まり文句はここでもあてはまります。個人情報保護に関し取締役会メンバーはコンプライアンス、倫理、企業戦略という3つの重要な相互に関連する問題を考慮する必要があります。そのために取締役は以下のことを考慮しなければなりません。

- 組織は国内外の多様な基準にどのように対処していますか。現在の個人データ保護規制を満たす上で現状のコンプライアンスプロセスはどの程度効果的ですか。

- 個人情報に関する法律や規制の遵守とは別に、今日的な視点と組織特有の視点から考えて、「責任ある」個人情報慣行とは何ですか。規制遵守の確保、正しいことを行うこと、またはその両方に観点で会社のデータの管理と運用を行っていますか。顧客のデータの保護と活用に関して自社のポリシーと基準は何ですか。取締役会の監視の役割はこれらの分野にどう対処すべきですか。

- 企業戦略の一環として組織で許容されるデータの種類は何ですか。機密データの不適切な使用を防ぐためにどのようなポリシーと境界線が設けられておりますか。

**積極的である：**取締役会は、「責任ある個人情報保護」ということが組織にとって具体的に何を意味するのかを理解する必要があります。ある取締役が指摘したように、取締役会には組織のデータと個人情報管理を監視するための基準、つまり「北極星」が必要です。取締役はリスク（組織を保護する）と戦略（イノベーションと組織の成長）のバランスに関してデータと個人情報保護を明確に理解する必要があります。

**重要なポイント —** 経営者と協力する上で最も効果的な取締役会は、データと個人情報保護の問題を理解し対処するために、事後対応ではなく、その監視活動に積極的に関与しています。したがって、取締役は自社のコンプライアンスプロセスが現在の個人データ保護規制をどのように満たしているかだけでなく、将来の個人データ保護義務を満たすのに十分な柔軟性があるかどうかにも疑問を持つ必要があります。

**ビジネス目的を理解する：**新しいテクノロジーの分野で組織がビジネスを成長させるために使用するプロセスと技術を理解し、収集したデータ（マーケティング、ビジネス開発、収益化など）をどのように使用するかを、取締役会は経営陣と協力して学ぶ必要があると合意しました。具体的には、収集した情報に対してどのようなビジネスを行っているか、またデータの収集と維持に起因するリスクおよびそれらのリスクの管理方法を理解する必要があります。情報収集の目的、収集プロセスおよびデータの利用を顧客に伝える方法を理解する上で、企業が収集しているすべての情報を本当に必要としているかどうかを取締役が問い合わせることもできます。

**重要なポイント —** 最終的に、「どれくらいのデータが多すぎるのか」という疑問に答えることに焦点を当ててください。組織はリスクを管理するためにデータ収集に制限を設けていますか。それとも、何らかの方法でそのデータが収益化に役立つかもしれないと考えて、法律や規制の遵守を前提とした上で可能なすべての情報を収集しますか。後者の場合、投資収益率（ROI）はデータ収集、管理の手間と関連リスクを価値のあるものにするのに十分ですか。もしそうならこのROIは収集されたデータの収益化から株主価値を促進する戦略に不可欠ですか。

**組織の外部を見る：**サプライチェーン内およびサードパーティプロバイダー間で重要データがある場所と管理方法を経営陣が確実に理解できるように、取締役会が監視する必要もあります。第 1、第 2、第 3 層のサプライヤー、個人を特定できる情報（PII）の外部処理者、その他の外部委託先等、サードパーティとの間で発生する個人情報保護とデータの問題は、究極的な責任追及のための出所を追求します。外部委託先がデータの問題を起こした場合、特定の企業とそのブランドが最終的に損害賠償責任を負います。従って、すべてのサードパーティが同じ個人情報保護基準で一貫して運用し、契約している組織のポリシーに従ってデータを維持することが重要です。

**重要なポイント —** サードパーティのリスク管理を効果的に実行できない組織はデータやコンプライアンス上の深刻な問題に直面する可能性があります。取締役会はベンダーやサードパーティが適切なリスク管理と監視プロセスを実施していることを適切なレベルのサポートを得て経営陣から保証を得る必要があります。

**データ集約（Data Aggregation：データ分析のためのデータベースからの抽出・集計・加工）の実施状況を検討する：**ラウンドテーブルの議論では、データの集約は組織が直面する可能性のある別の倫理的・法的問題であり、データへのアクセスを他の組織に販売する場合の問題に特別に言及しました。個々のデータ収集とは異なり、データの集約は個々の消費者データや個人情報に影響を与えません。取締役会は経営陣と協力して、データ集約に関する活動とパラメータを定義し、組織のリスクプロファイルが変化するかどうかを確認する必要があります。また、

集約したデータに PII や法的に保護された消費者情報が含まれていない可能性があるので、別の倫理的配慮が必要となる場合もあります。したがって、取締役会は、倫理、コンプライアンスおよび望ましいリスクプロファイルに関する会社の合意された見解に照らして、データ集約に関する組織の戦略と実施状況を理解する必要があります。

**重要なポイント** — データ集約は正しいことですか。個人情報保護に関する法律や規制を遵守する上でデータ集約のプロセスはどの程度効果的ですか。データが適切にまとめられ匿名化されていますか。これらの考慮事項は、組織が収集するデータを使用する際に会社の価値観、倫理、プロセスや目的を理解することの重要性を強調しています。

多くの重要なポイントなど、このラウンドテーブルの詳細については、プロティビティのイベントの包括的な要約をwww.protiviti.com/US-en/insights/responsible-privacy-boardでお読みください。

### 取締役会の考慮事項

会社の業務に内在するリスクに基づき、取締役会は上記の議論で指摘された重要なポイントを考慮しましたか。

## プロティビティの支援

プロティビティは、多くの国でクライアントの個人データ保護プログラムをサポートするグローバルな組織です。日本の個人情報保護法、米国の1996年の健康保険の可搬性と説明責任に関する法律(HIPAA)、カリフォルニア消費者プライバシー法(CCPA)、その他の州または連邦ベースの規制、EUにおける一般データ保護規則(GDPR)や今後の eプライバシー規制に対して、また、個々のEU加盟国やブラジル、インド、中国、カナダ等のさまざまな国において、プロティビティは企業が効果的かつ効率的な個人情報保護対応の構築と実施を支援します。私たちは、準備状況を評価し、企業が個人データ保護の態勢をよりよく理解し、持続可能で効果的な個人情報プログラムを推進するために、必要な人・プロセス・技術をカバーする費用対効果の高いコンプライアンスソリューションを設計することで、個人情報保護とセキュリティ管理をサポートします。

IT、法務、コンプライアンス、マーケティング、ビジネスユニットなどのグループと連携して、国内およびグローバルに焦点を当てたデータ個人情報保護コンプライアンスプログラムの開発、実施、維持を支援しています。当社のサービスには以下が含まれます。

- **規制の解釈** — 分析とアドバイス
- **高度なデータ管理技術** — データと処理方法の自動検出など
- **主要な活動におけるギャップの改善** — 第三者のリスク、個人データに関する権利、データガバナンス、プライバシー通知の設計と実装など
- **コンプライアンスソリューション** — 効果的なサイバーセキュリティと個人情報保護プログラムのための、人・プロセス・テクノロジーの統合
- **コンプライアンス管理** — コントロールの継続的なモニタリングと維持

私たちはコンプライアンス活動のあらゆる段階でクライアントをサポートします。当社の組織は、さまざまなプラクティスやバックグラウンドを持つグローバルコンサルティングの人材を統合し、グローバルセキュリティと個人情報保護の実践やデータおよび分析チームの機能専門知識、ロバートハーフリーガルの法的および個人情報保護サポートなど、お客様の国際的な個人データ保護ニーズに対応するためのカスタマイズされたチームを提供します。



protiviti®