ABeam Consulting®
Build Beyond As One.

ABeam Security® Privacy Regulation Consulting Service

# ABeam Security® プライバシー法対応評価と対策支援サービス

**消費者のプライバシー保護に係る各種法規制への対応状況・課題点を可視化し、企業の法令違反リスクの低減ならびに企業価値向上に貢献**

近年、消費者のプライバシー保護に係る各国の法規制が厳格化・複雑化の傾向にあり、知らぬ間に法令違反を犯すことで高額違反金が発生し、かつブランド価値が低下するリスクが高まっています。本サービスは、規範・法律、プロセス、テクノロジー、人・組織の観点で、各種法規制の要求事項と対応状況のギャップ分析を実施し、対策を支援することで、法令違反リスクの低減ならびにデータ利活用促進による収益拡大に寄与します。

## 各種法規制対応に係る落とし穴

各国が策定を進めるプライバシー法規制の模範となりつつあるGDPR（一般データ保護規則）・CCPA（カリフォルニア州消費者プライバシー法）は、消費者のプライバシー保護という点では共通ですが、策定目的が異なるため、厳格さの方向性が異なります。GDPRは、自身の知らない範囲で個人データが使用されないよう、EEA（欧州経済領域）域外へのデータ移転を厳格に取り締まる等、データの保護を強調しています。一方CCPAは、消費者が自身の個人データを管理するための権利（個人データの開示・削除請求権等）を強調しています。このような目的を理解せず法制対応を進めると、法律の要求事項に対する逐次対応の域を超えず、法改正を見越した解決にはつながりません。

### ■ GDPR 主な要求事項と対応に係る落とし穴の例

| | |
|---|---|
| 成立目的 | DX推進によりEEA域内・域外への個人データ流通量が増加し、自身の知る範囲外で個人データが使用されるリスクが上昇。当該リスクを低減するための各種保護措置をとりつつ、域内・域外での個人データの更なる流通を促進。 |
| 主な要求事項と対応の落とし穴 | **1. データ保護バイデザイン（データ保護も要件とした設計思想）の義務化**<br>要求事項への表面的な対応（開発初期段階でプライバシー保護を検討するようルール化）のみで満足し、法規制の意図の理解・自社のあるべき姿の明確化が不十分となり、ルールの形骸化や頻繁なルール改正が発生。<br>**2. 個人データの域外移転は原則禁止**<br>要求事項への表面的な対応（システム的な制御等）のみで満足し、法規制の目的を自社の要件として捉えず、移転が許容される条件の確認プロセス等が未整備となる等、法改正時の対応が鈍足化。<br>**3. データ侵害時の報告義務化**<br>要求事項への表面的な対応（データ侵害時の報告迅速化に向けた個人データ所在整備等）のみで満足し、法規制が求める精度の管理がなされず、データ侵害の未然防止策の検討等が疎かになる。 |

### ■ CCPA 主な要求事項と対応に係る落とし穴の例

| | |
|---|---|
| 成立目的 | 企業による個人データ使用量の急増等を受け、米国カリフォルニア州在住の消費者自身が個人情報を管理する必要があるという機運が高まったため、消費者が自身の個人データを自分で管理するための権利を明文化。 |
| 主な要求事項と対応の落とし穴 | **1. 消費者の権利行使（データ開示・削除等）への対応義務**<br>要求事項への表面的な対応（消費者向け窓口開設等）のみで満足し、法規制の意図が顧客の権利保護であることを理解せず、法改正や新サービス開発の度に消費者向け窓口が乱立し、消費者目線の権利強化と逆行。<br>**2. 消費者要求の検証や記録管理義務**<br>要求事項への表面的な対応（消費者要求の記録）のみで満足し、消費者要求の軽視はブランド低下につながることを認識しないため、消費者要求に係る運用改善が見込めない。<br>**3. 権利を行使した消費者への差別禁止**<br>要求事項への表面的な対応（差別禁止のルール化・周知等）のみで満足し、データ削除等は消費者が期待する当然の権利であるという意識が欠如し、ルールの形骸化や頻繁なルール改正が発生。 |

## 企業で想定される法規制対応上の課題

各法律の要求事項は複雑・広範なため、網羅的に対応するには、規範・法律、プロセス、人・組織、テクノロジーといった４つの観点でバランスの取れた対策が求められます。このため、法規制対応における各社の課題として、「システム改修、ルール整備、体制構築等が個々別々で遂行されており、対応の整合性が取れているか不安」「社内規定は一新したが、経営層含めプライバシー保護に係る社員の認識が低く、ルールや手順の不順守が多発」等があり、４つの観点全てで十分な対応を実現するには、専門家の知見が必要であると想定されます。

| ① 規範・法律 | ② プロセス | ③ 人・組織 | ④ テクノロジー |
|---|---|---|---|
| 消費者要求への対応形式・期限等が法律間で異なり網羅的に対応できているか不安 | 個人データの安全管理措置は見直したがシステムの利用手順やフローが未整備で業務が俗人化 | 規定は整備したが社員のプライバシー保護に対する認識が浅くルールが形骸化 | ■ 個人データに対する必要十分な安全管理措置が取られているか不安<br>■ 過剰投資の不安 |

## サービス概要

GDPR・CCPA・個人情報保護法への対応状況を条文単位で評価し、課題を網羅的に洗い出したうえで、課題への対応策の策定ならびに解決を支援します。これにより、法律違反となることによる社会的信頼性の損失リスク等を低減しつつ、個人データ利活用の促進による企業収益拡大に貢献します。

## 特徴①　「規範・法律」「プロセス」「人・組織」「テクノロジー」の観点で全方位的に評価

各種法規制への対応状況を評価する際は、企業運営に係る要素を網羅する観点でのバランスを考慮する必要があります。バランスが欠如すると、「セキュリティ対策ツールを導入したが利用フローが未整備」「情報セキュリティに掛かる社内規定を整備したが従業員に浸透していない」等、片手落ちの対応となるリスクがあります。本サービスは、「規範・法律」「プロセス」「人・組織」「テクノロジー」の観点で対応状況を評価するため、全方位的な課題の洗い出し・対応策の策定が可能となります。

### Organization（人・組織）

☑ 個人情報の収集・利用・変更・削除、データ侵害時の関係者報告、海外へのデータ移転等の業務遂行に必要な組織内の役割・権限は明確か。
☑ 整備したプロセスとルールは社内に浸透しているか。

### Technology（テクノロジー）

☑ 個人情報の収集や利用における安全管理措置（仮名化・暗号化・アクセス制御等）は完備されているか。
☑ 個人データ侵害時に迅速に対応できるよう、ログ取得の仕組みや個人データの所在等は整備されているか。

### Regulations（規範・法律）

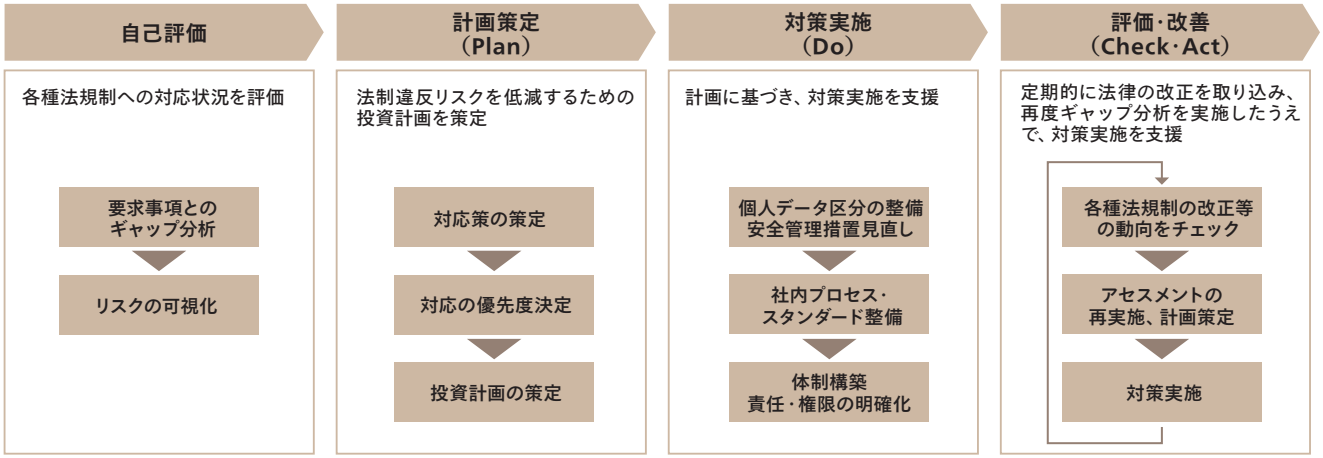
☑ 個人情報の収集・利用・変更・削除、データ侵害時の関係者報告、海外へのデータ移転に関して従業員が順守すべきルールや標準は整備されているか。
☑ 消費者要求（データ開示・削除等）への対応に係る各種ルール（回答期限、禁止事項等）は明確か。

### Process（プロセス）

☑ 個人情報の収集・利用・変更・削除、データ侵害時の関係者報告、海外へのデータ移転等の
☑ 業務遂行に必要なプロセス・手順は整備されてるか。消費者要求（データ開示・削除等）への対応プロセス・手順は整備されているか。

## 特徴②　評価のみで完結するのではなく、リスク低減策の策定、対策実施まで支援

各種法規制への対応状況を評価するのみでは、机上の空論で終わることとなります。アビームコンサルティングでは、評価の結果明らかになったリスクへの低減策の策定、ならびに対策の実施までサポートすることで、より実態に即した本質的な課題解決や、真に実のあるリスク低減・データ利活用の促進を実現します。




【想定期間の目安】　自己評価：1ヶ月～(整備状況を含む現況により変動)、計画策定以降：自己評価の結果により変動

## サンプルイメージ

自己評価シートサンプル：規範・法律、プロセス、人・組織、テクノロジーの観点で、各法規制への対応状況を網羅的に評価

**プライバシー法制対応チェックシート**

| 大分類 | 中分類 | 小分類 | 各規制における遵守すべきポイント | Security Quadrantの4観点 | 具体的なチェック内容 | 各チェック項目への準拠有無。 | 各チェック項目への準拠状況の詳細 | チェック結果の証跡となる文書 | 監査チェック項目において参照した法規制、及び法規制内の項目。チェック項目から法規制の項目を逆引きする際に使用する想定 |
|---|---|---|---|---|---|---|---|---|---|

| カテゴリ | | | タイトル | チェック観点・内容 | | チェック結果 | | | 参照法規制 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 大分類 | 中分類 | 小分類 | | チェック観点 | チェック内容 | 対応状況（未対応、対応中、対応済） | 対応状況詳細 | 証跡 | GDPR | CCPA 条文 | CCPA 規則 | 改正個人情報保護法 |
| データの保護・利活用 | 個人情報の取扱前準備 | データ保護影響調査 | データ保護影響調査の実施義務 | ①テクノロジー | 個人情報の取扱いにおいて新たな技術を用いる場合等で、個人の権利等へ高いリスクを発生させる恐れがある場合、その取扱いによる個人データ保護への影響評価が必要だが※、実施可能なよう仕組みは整備されているか。（例：個人情報の取扱いによるリスクを計算できるようロジックや仕組みは整備されているか、リスクを軽減する安全管理措置（アクセス制御や暗号化等）は整備されている | | | | 第35条1,2,3,7、第36条 | | | |
| データの保護・利活用 | 個人情報の取扱前準備 | データ保護影響調査 | データ保護影響調査の実施義務 | ④規範・法律 | 個人情報の取扱いにおいて新たな技術を用いる場合等で、個人の権利等へ高いリスクを発生させる恐れがある場合、その取扱いによる個人データ保護への影響評価が必要だが、社内の各種規定やポリシーは当該義務と整合が取れているか（例：データ保護影響評価の実施が必要となる基準、評価すべき項目は明記されているか） | | | | 第35条1,2,3,7、第36条 | | | |
| データの保護・利活用 | 個人情報の取扱前準備 | データ保護影響調査 | データ保護影響調査の実施義務 | ②プロセス | 個人情報の取扱いにおいて新たな技術を用いる場合等で、個人の権利等へ高いリスクを発生させる恐れがある場合、その取扱いによる個人データ保護への影響評価が必要だが、社内のプロセスや手順は当該義務と整合が取れているか（例：新たに個人情報を取扱う場合のデータ保護影響評価の実施要否の検討プロセス、評価自体の実施プロセス・手順は整備されているか） | | | | 第35条1,2,3,7、第36条 | | | |

**アビームコンサルティング株式会社**
www.abeam.com