1　個人情報保護とプライバシーの考え方（前提）

【個人情報保護とプライバシー】

保護する本来の目的は、**「個人のプライバシーの尊重」**と**「権利を守る」**ためにあり、個人情報という**「もの」**を守るだけでは達成できないということを認識しなければなりません。

プライバシーに関する問題については、個人情報保護法を順守しているか否か（コンプライアンス）の点を中心に検討されてきました。しかし法令を順守していても、本人への差別、不利益、不安を与えることがあり、批判を避けきれず炎上し、企業の存続に関わるような問題として顕在化するケースが見られます。

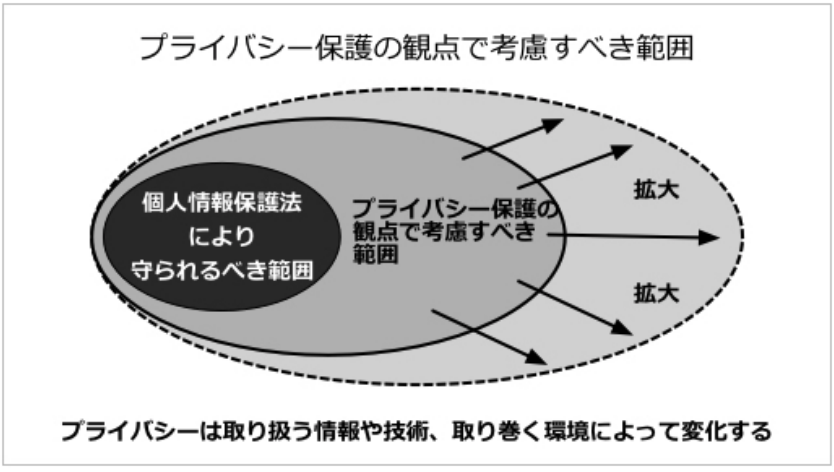
また、保護法は３年ごとの見直しをしながら最適化していこうとしていますが、この変化の激しい時代に、法さえ守っていればよいという考え方で、本当に目的を達成できるでしょうか。

過去にも、違法薬物に法で指定されてなければ、効能が同じでもかまわないという事件がありました。法律は変化のスピードに追いついていけるのでしょうか。また、何でも法律で規制してしまうことによって、様々な弊害も出てくるように思われます。

私たちが、法令遵守する際には、**法の本来の目的**を理解し、取り組まなければなりません。

そのためには、「もの」としての個人情報という範囲を超えて、**「プライバシーの権利」を保護できる組織文化・倫理観**を持ち、信頼関係を維持していく活動にすることが大切です。

法律改正によってやらなければならない事が増えたというネガティブな発想ではなく、誰からも信頼されるために、組織・人の価値を向上させるポジティブな取組みと捉えましょう。



●プライバシーは保護するのではなく尊重するもの（ルールの前に正しい倫理観が必要）
・プライバシーは「権利」であり、「もの」ではない

・個人情報保護法は、「もの」として定義できる個人情報を保護することで、プライバシーという権利を尊重することを目的としている

●個人情報保護法と社会的認知（プライバシー尊重）のギャップ
・個人情報保護法の定義は、拠り所となる判断基準（ものさし）を設けたもの
・社会的認知は、法律の定義と必ずしもレベルが同一ではなく、広いもの

●考え方と行うべきこと
・お客様の信頼を得るためには？（Why：プライバシー尊重、倫理観醸成）
・具体的に、どんなことをしなければいけないか？（How：保護ルールの整備と運用）

●法律やガイドラインのルールを守ることは大変ですが・・・
・「ルールを守ること ＝ 日常生活で他人（顧客）に信用されること」と置き換えて考えてみることで、個人情報保護が特別なことではなく、人に誤解を受けないため、信頼を得るための当たり前の行為と考えることもできます。

【プライバシーと個人情報の違和感】

●「プライバシーの侵害」と感じるときは、どんな時でしょうか？
・全く知らない会社からDMが来た／わけのわからない会社から勧誘の電話があった
・友人が、一緒に遊びに行った時に撮った写真を位置情報付きでSNSに投稿した
・SNSに根も葉もないことを投稿され、精神的被害を受けた

●個人情報の取扱いで不便に感じることは、どんな時でしょうか？
・子供のクラスの緊急連絡網が配布されなくなった
・セミナーやイベントで作成した連絡先リストを、終了後にどう扱うべきか悩ましい

2　改正個人情報保護法が施行される背景

【目的：利活用促進と本人の権利強化】

データドリブン時代と言われる現代では、個人情報の有効活用は必要不可欠ですが、法律での個人情報の取扱いについては曖昧な部分が多く、機密性が強調されるあまり、本来あるべき個人情報の利活用によるサービス提供や顧客満足の向上に歯止めがかかっていました。

そのため改正では、利用法の曖昧さを解決するために**「仮名加工情報」「匿名加工情報」「個人関連情報」**等を新たに定義することで個人情報の有効活用を促進しようとしています。

しかし、安全な利活用のためには、リスクを適切にコントロールする必要があります。

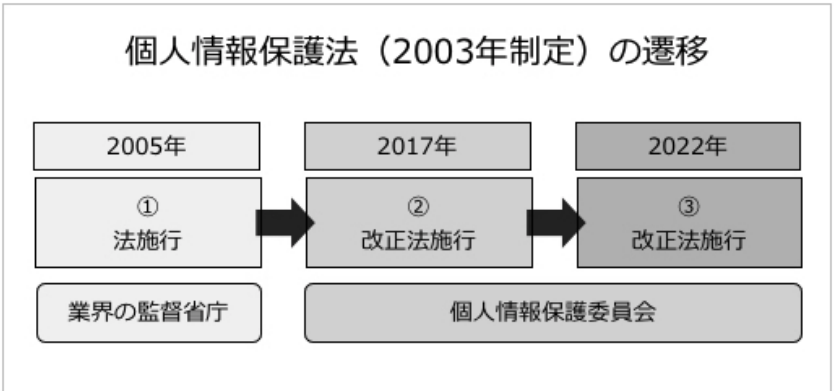
従来から名簿事業者間の無責任な取引で、漏えいしても流出元が不明であったり、第三者提供等で自分の情報がどう使われているか、正しいのか等、個人の権利利益が守られているんだろうかという不安がつきまといました。

それらの不安に対しては、**第三者提供制限や委員会への報告、本人の権利強化による請求権の拡大、罰則強化**等の対策が盛り込まれました。

【改正個人情報保護法施行と推移】

2020年6月12日に「個人情報の保護に関する法律等の一部を改正する法律」が公布され、**2022年4月1日**に施行されます。今後も３年毎の見直しを経て改正が行われる予定です。その都度、従来の個人情報保護活動に追加して、改正法への対応をすることになります。

2003年の個人情報保護法制定、2005年の施行以来状況の変化に応じて改正、施行されています。以前は各々の監督省庁管轄でしたが、2016年には、独立した行政機関として「個人情報保護委員会」が設置され、統括して管轄しています。



・2003年５月23日：個人情報保護法制定（一部施行）
・2005年４月１日：個人情報保護法施行（全面施行）
・2017年５月30日：改正個人情報保護法施行（改正）
・2022年４月１日：改正個人情報保護法施行（改正）

また最近では、ビジネスのグローバル化による個人情報保護に対する大きな流れとして、地域毎の法令遵守だけではカバーしきれないプライバシーの権利を、リスクベースの評価によって、**プライバシーガバナンスや情報セキュリティガバナンスという自律的な活動**で対策し、顧客との信頼関係醸成の視点から対応しようという取り組みにシフトしています。

【個人情報保護委員会とは】

個人情報保護については、従来各事業者を管轄する省庁（経産省や厚生省等）が管轄していましたが、2016年に個人情報保護委員会が設置され管轄することになりました。

委員会は、個人情報／特定個人情報（マイナンバー）の有用性に配慮しつつ、その適正な取扱いを確保するための独立性の高い機関であり、個人情報保護法および番号法に基づき、個人情報の保護に関する基本方針の策定・推進や監督、国際協力等を行います。

また、具体的な法の遵守方法として、個人情報の保護に関する法律についての各種ガイドラインを公表しています。日本企業は個人情報保護関連の諸対応について以下のガイドライン等を中心に対応を検討し、実施することになります。

（個人情報保護委員会のガイドライン例）

・通則編（全般）
・第三者提供時の確認・記録義務編
・匿名加工情報編
・外国にある第三者への提供編
・認定個人情報保護団体編　等

【日本のプライバシー保護ガイドライン】

日本では個人情報保護法や保護委員会のガイドラインの他に、各業界でユーザーのプライバシーを保護するためのガイドラインがあります。

例えば、広告業界ではJIAA（日本インタラクティブ広告協会）が定めたJIAAガイドラインがあり、プライバシーポリシーや行動ターゲティング広告について、運用のルールを定めています。

つまり、日本において企業は、まず個人情報保護法による規制を正しく理解すること、次いで法律以外の業界自主規制として各種ガイドラインがあることを覚えておきましょう。

【グローバルでのプライバシー保護規制】

プライバシー保護については、以前からEUが中心となってグローバルに議論され、各国が個人およびプライバシーの権利の重要性から、以下のような各種規制を強めています。

- 1980年
  OECDプライバシー８原則（経済協力開発機構／EU、米、日など38ヶ国）
- 1995年
  EUデータ保護指令
- 2018年
  一般データ保護規則＝GDPR: General Data Protection Regulation
- 2020年
  消費者プライバシー法＝CCPA: California Consumer Privacy Act of 2018

また、グローバルネットワーク企業やプラットフォーマ（GoogleやApple等）もCookieの利用規制などの技術的規制を強めており、ビジネス、プライベートでも意識が高くなっています。

日本国内でもグローバルなイベントが開催・予定されていますので、大企業やグローバル企業だけでの問題ではなく、サプライチェーンを構成する中小事業者にも大きな影響がありそうです。

3　法改定の考え方と視点

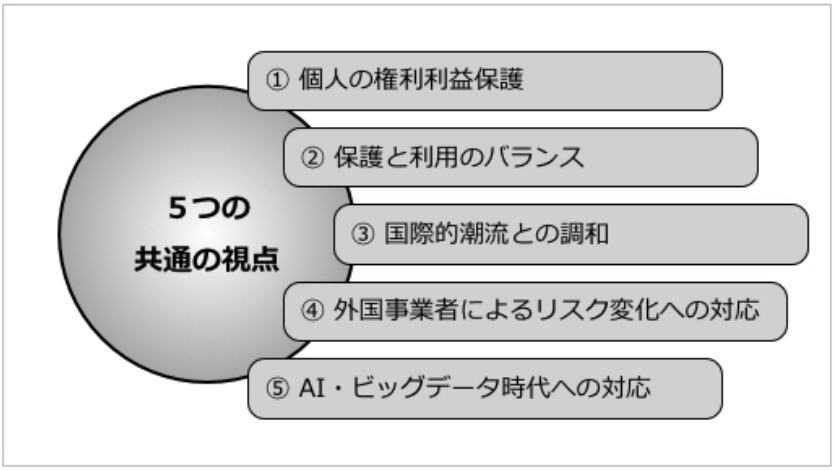
【３年ごとの見直しで変化に対応】

個人情報保護法は、個人情報を取り扱う企業が守らなければならない義務を規定しています。しかし、ネットワークが急速に発展する中で、個人情報の価値も高くなり、その**取り扱う環境やリスクも大きく変化**しているため、見直しが必要となっていました。

個人情報保護委員会（PPC: Personal Information Protection Commission）は、2015年の個人情報保護法の改正以来、社会・経済情勢の変化を踏まえて、2019年に公示された「３年ごと見直しに係る検討の着眼点」によって、個人情報保護法の見直しと改善を進めています。

【５つの共通の視点】

今回の改正は、見直しの過程で得られた「共通の視点」（社会の様々な変化）を反映し、個人情報保護委員会は視点として次の５つを示しています。



変化する環境・リスクの下で、事業者は個人情報を取り扱う際に、個人（本人）の権利利益保護のために説明責任を果たし、本人の予測可能な範囲内で適正な利用がされるように、環境を整備していくことを重要課題として改正の視点（考え方）を示しています。

（１）個人の権利利益保護（本人の関与強化）

情報を提供する個人の、自らの情報の取扱いに対する関心や、関与への期待が高まっており、個人情報保護法第１条の目的に掲げている**「個人の権利利益を保護」**するために必要十分な措置を整備すること に配意しながら制度を見直す必要がある。

（２）保護と利用のバランス（ビジネス視点）

平成27年改正法で特に重視された保護と利用のバランスをとることの必要性は、引き続き重要であり、個人情報や個人に関連する情報を巡る技術革新の成果が、**経済成長等と個人の権利利益の保護**との両面で行き渡るような制度を目指すことが重要である。

（３）国際的潮流との調和（グローバル視点）

デジタル化された個人情報を用いる多様な利活用が、グローバルに展開されており、国際的な制度調和や連携に配意しながら制度を見直す必要がある。

（４）外国事業者によるリスク変化への対応（ネットワークビジネス対応）

海外事業者によるサービスの利用や、国境を越えて個人情報を扱うビジネスの増大により、個人が直面するリスクも変化しており、これに対応する必要がある。

（５）AI・ビッグデータ時代への対応（情報技術の進歩対応）

AI・ビッグデータ時代を迎え、個人情報の活用が一層多岐にわたる中、本人があらかじめ自身の個人情報の取扱いを網羅的に把握することが困難になりつつある。

4　有効活用のためのWhy, What, How

これからは、今以上に個人情報含む情報の利活用能力がビジネスを大きく左右すると考えられます。
そして、この変化の時代では単に個人情報保護法に従うだけではなく、そこに存在する**「プライバシーの権利」を危うくするリスク**について、状況に応じた判断と対策を実施し、情報提供者に納得してもらえる戦略・方針を定めることが価値ある活動を生み出すことになります。

1）Why（目的）：プライバシーの尊重（何が求められているのか／法を超えて）

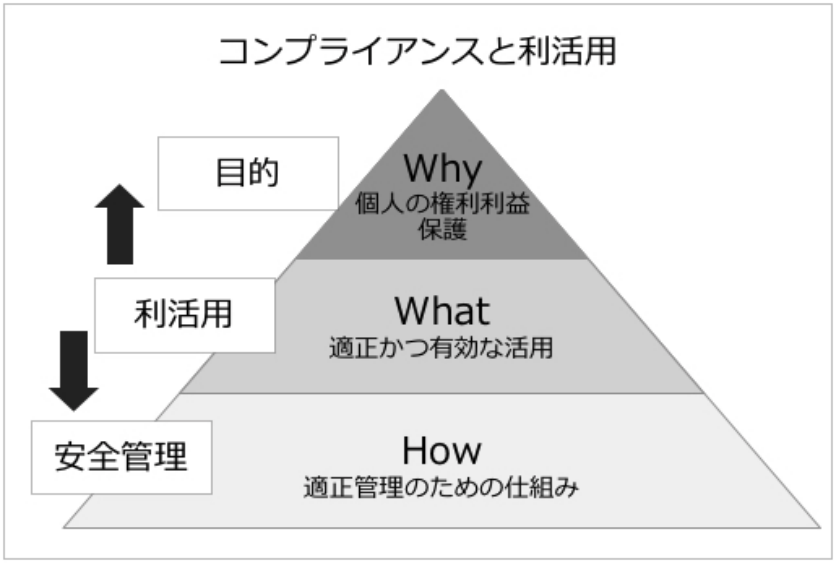
・顧客や相手のプライバシーの権利を尊重し、信頼関係を構築すること。
・個人の私生活に関する事柄やそれが他から隠されており干渉されない状態を要求する権利、を尊重すること。（忘れ去られる権利）

2）What（利活用のために）：社会的信用の醸成（社会的認知）

・組織は個人情報をどう活用するのか？（戦略・方針が必要）
・法の遵守だけでなく、プライバシーにも配慮する。（多様な変化とリスクへの対応）
・組織は周りから認められる必要があり、それは法を遵守している事だけではない。（ガバナンス・組織文化・信頼性・倫理観の醸成）

3）How（方法）：法遵守／コンプライアンス（責務：組織としての最低ライン）

・個人情報保護法 = 組織が国内で活動を行う際に、個人情報を適正に取扱うためのルール（何をして良く、何をしてはいけないかの定義）を守る。
・個人情報保護法は、組織に遵守することが要求され、個人情報を取り扱う組織にとっては当たり前の責務と捉える。



5　個人情報漏えい事故の影響

私たちは、個人情報保護法遵守のためだけではなく、組織で働く人の責任として預かった情報を大切に守るのは当然の義務です。

しかし、日常的に情報漏えい事故が起こっている現実があります。これらの事故（インシデント）は、法による罰則だけではなく、組織に多大な損害を及ぼすことを認識しなければなりません。

組織には法令遵守だけではなく、変化するリスクを常に捉え、重要な情報資産を適切にコントロールできる**マネジメントとガバナンス能力**が求められています。

脅威は刻々と変化しており、攻撃者は国家組織から個人にまで広がっており、**サイバー攻撃や内部不正、オペーションミスなど様々な脅威と脆弱性**に対処しなければなりません。

【インシデントによる組織への影響（損害）とは】
１回の事故でも、漏えい数や直接的な損害と間接的な損害を含むと、事業の継続に大きな影響があることを認識しておきましょう。

インシデントによる損害

費用損害（事故対応）	被害発生から収束に向けた各種事故対応に関して自社で直接、費用を負担することにより被る損害（下記に該当しないもの）
賠償損害	情報漏えいなどにより、第三者から損害賠償請求がなされた場合の損害賠償金や弁護士報酬等を負担することにより被る損害
利益損害	ネットワークの停止などにより、事業が中断した場合の利益喪失や、事業中断時における人件費などの固定費支出による損害
金銭損害	ランサムウェア、ビジネスメール詐欺等による直接的な金銭の支払いによる損害
行政損害	個人情報保護法における罰金、GDPRにおいて課される課徴金などの損害
無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、金銭の換算が困難な損害

【個人情報漏えいインシデントの状況と賠償コスト】
漏えい規模によっても異なりますが、日本では１件あたりの漏えい事故で５～６億円もの損害賠償額となっています。また、一人当たりの賠償額も約３～４万円との調査結果があります。（JNSA調査）

個人情報漏えいインシデント概要（2018年調査）

	2018年調査結果	年平均比較 (2005～2017年)
漏えい人数	561万3,797人	1,381万7,110人
漏えい件数	443件	1,231件
想定損害賠償総額	2,684億5,743万円	5,340億1,627万円
漏えい人数／件	1万3,334人	1万4,259人
平均想定損害賠償額／件	6億3,767万円	5億6,033万円
平均想定損害賠償額／人	2万9,768円円	3万9,178円

個人情報漏えい損害賠償金コスト

自社管理の個人情報	情報漏えいの被害者個人から慰謝料等についての損害賠償請求

調査年	1人あたり平均想定損害賠償額（JNSA調査）
2016年	31,646円
2017年	23,601円
2018年	29,768円
3年平均	28,308円

他社から管理委託を受けた個人情報	委託元企業が実施した各種事故対応に要したコストについて、損害賠償請求「求償」がなされる 委託元にも一定の責任があるとして過失相殺が認められるケースもあるが、損害賠償金の額は中小企業であったとしても数千万～数億円

【主な関連法令と罰則】

法令違反罰則については、日本に比べてEUや米国はかなり高額になります。グローバル対応時には十分な注意が必要となります。

関連する主なプライバシー関連法令と罰則

日本	個人情報保護法	データベース等不正提供罪、委員会による命令違反の場合、最大1億円
EU	GDPR	違反内容により次の①または② ①「情報漏えいの発生時に監督機関へ72時間以内に報告しなかった」「データ保護責任者の任命が義務付けられているにもかかわらず任命していなかった」などの場合最大1,000万ユーロまたは全世界年間売上高の2%のいずれか高い額 ②「個人データの処理に関する原則に違反した」「監督機関からの命令に従わなかった」などの場合最大2,000万ユーロまたは全世界年間売上高の4%のいずれか高い額
米国	CCPA	消費者１名／最大2,500ドル（故意7,500ドル）（カリフォルニア州）