日本DPO協会
第11回オンライン例会

令和２年改正個人情報保護法について

～漏えい等の報告・本人通知、不適正な利用の禁止等～

令和４年２月２４日

●本資料は、令和２年改正個人情報保護法に関する法律・政令・規則・ガイドライン・Ｑ＆Ａ等の一部について、その概要等をまとめたものであり、事業者の義務や例外規定等の全てを記載したものではありません。

●令和２年・３年改正個人情報保護法のより詳細な内容については、個人情報保護委員会のＨＰ等をご参照下さい。
☞ https://www.ppc.go.jp/personalinfo/

●令和４年４月１日以降は、令和３年改正法による各規定が適用されます。なお、本資料中の条文番号は、便宜上、令和２年改正法によるものと、令和３年改正法（のうち令和４年４月１日施行関係※）によるものについて、例えば、前者を§28、後者を［§33］として記載しています。

※デジタル社会形成整備法第50条による国の行政機関、独立行政法人、学術研究機関等関係
（同第51条による地方公共団体等関係は令和５年春頃施行予定）

Ⅰ．はじめに

※総論のおさらい

３年ごと見直しに当たっての「５つの視点」

個人の権利利益の保護

- 「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

技術革新の成果による保護と活用の強化

- 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に行き渡ること

国際的な制度調和・連携

- 国際的な制度調和や連携に配意すること

越境データの流通増大に伴う新たなリスクへの対応

- 海外事業者によるサービスの利用や、個人情報を扱うビジネスの国境を越えたサプライチェーンの複雑化などが進み、個人が直面するリスクも変化しており、これに対応すること

ＡＩ・ビッグデータ時代への対応

- 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、事業者が本人の権利利益との関係で説明責任を果たしつつ、本人の予測可能な範囲内で適正な利用がなされるよう、環境を整備していくこと

令和２年改正法の概要

１．個人の権利の在り方

① **利用停止・消去等の個人の請求権**について、一部の法違反の場合に加えて、**個人の権利又は正当な利益が害されるおそれがある場合等にも拡充**する。

② **保有個人データの開示方法**（現行、原則、書面の交付）について、**電磁的記録の提供を含め、本人が指示できる**ようにする。

③ 個人データの授受に関する**第三者提供記録**について、**本人が開示請求できる**ようにする。

④ ６ヶ月以内に消去する**短期保存データ**について、保有個人データに含めることとし、**開示、利用停止等の対象**とする。

⑤ **オプトアウト**規定※により第三者に提供できる個人データの範囲を限定し、**①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外**とする。

（※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

令和4年4月以降に同規定による提供を行う場合は、令和3年10月１日より届出可能。

２．事業者の守るべき責務の在り方

① 漏えい等が発生し、個人の権利利益を害するおそれが大きい場合※に、**委員会への報告及び本人への通知を義務化**する。

（※）一定の類型（要配慮個人情報、不正アクセス、財産的被害）、一定数以上の個人データの漏えい等

② **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

３．事業者による自主的な取組を促す仕組みの在り方

① 認定団体制度について、現行制度※に加え、**企業の特定分野(部門)を対象とする団体を認定できるようにする。**

（※）現行の認定団体は、対象事業者の全ての分野（部門）を対象とする。

４．データ利活用の在り方

① 氏名等を削除した**「仮名加工情報」を創設**し、内部分析に限定する等を条件に、**開示・利用停止請求への対応等の義務を緩和**する。

② 提供元では個人データに該当しないものの、**提供先において個人データとなることが想定される「個人関連情報」の第三者提供**について、**本人同意が得られていること等の確認を義務**付ける。

５．ペナルティの在り方　※令和2年12月12日より施行

① 委員会による命令違反・委員会に対する虚偽報告等の**法定刑を引き上げる**。

② 命令違反等の罰金について、法人と個人の資力格差等を勘案して、**法人に対しては行為者よりも罰金刑の最高額を引上げる**(法人重科)。

６．法の域外適用・越境移転の在り方

① 日本国内にある者に係る個人情報等を取り扱う外国事業者を、**罰則によって担保された報告徴収・命令の対象**とする。

② 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

※「７．その他」として、利用目的の特定、個人データの取扱いの委託及び公表等事項について、個人情報の保護に関する法律施行令等で規定

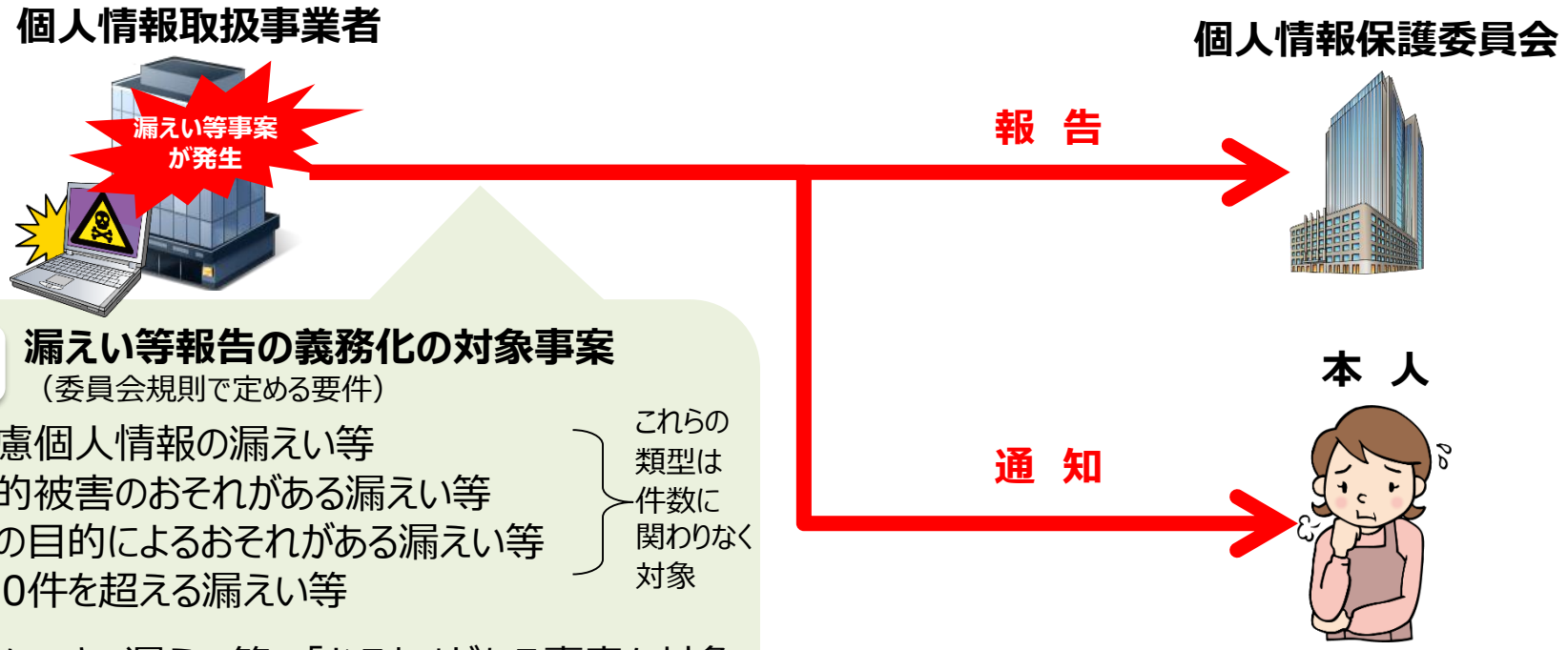
Ⅱ．令和２年改正法（各論）について

漏えい等の報告・本人通知、不適正な利用の禁止等～

漏えい等報告等の義務化

●漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、**委員会への報告及び本人への通知を義務化**する。

現　行	改正後
個人情報保護委員会に報告及び本人通知するよう**努める**（委員会告示）	漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、**個人情報保護委員会への報告及び本人への通知を義務化**する（§26）



漏えい等報告の義務化の対象事案
（委員会規則で定める要件）

- 要配慮個人情報の漏えい等
- 財産的被害のおそれがある漏えい等
- 不正の目的によるおそれがある漏えい等
- 1,000件を超える漏えい等

これらの類型は件数に関わりなく対象

※各類型につき、漏えい等の「おそれ」がある事案も対象。

漏えい等報告等の義務化

テーマ	法・政令・規則の概要	ガイドライン・Q&Aの概要
①漏えい等の報告・本人通知 §22の２［§26］	漏えい等が発生し、**<u>個人の権利利益を害するおそれがある場合</u>**に、**<u>委員会への報告及び本人通知を義務化</u>**する **<u>報告対象</u>**：①要配慮個人情報、②財産的被害が発生するおそれがある場合、③不正アクセス等故意によるもの、④1,000人を超える漏えい等を報告対象とする **<u>委員会への報告</u>**：速報と確報の二段階。事態の発生を認識した後、速やかに速報を求めるとともに、30日（上記③の場合は60日）以内に確報を求める	• **<u>委員会への報告を要する事態</u>**について、事例を含め解釈を具体的に記載するとともに、報告を要しない「高度な暗号化等の秘匿化がされている場合」の考え方、**<u>委員会への速報・確報の時間的制限</u>**の考え方、本人への通知が必要な事態等を記載 ➢ 財産的被害が発生するおそれがある漏えい等に該当する事例…ECサイトからクレジットカード番号が漏えいした場合 ➢ 速報の時間的制限の目安として、事態の発生を知った時点から概ね3日～5日以内（確報については、規則において原則30日以内と規定） など

漏えい等報告等の義務化

？ 漏えい等報告はどのような事態で行う必要がありますか？

類型	報告を要する事態
要配慮個人情報の漏えい等	従業員の健康診断等の結果を含む個人データが漏えいした場合
財産的被害のおそれがある漏えい等	・送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合 ・個人データであるクレジットカード番号のみの漏えい ※住所、電話番号、メールアドレス、SNSアカウント、銀行口座情報といった個人データのみの漏えいは、直ちにこれに該当しない
不正の目的によるおそれがある漏えい等	不正アクセスにより個人データが漏えいした場合
1,000件を超える漏えい等	システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が1,000人を超える場合

？ 漏えい等報告について、報告の期限はどのようになっていますか？

速報と確報の二段階で行う必要があります。

	時間的制限	報告内容
速報	報告対象の事態を知ってから「速やかに」（個別の事案によるものの、当該事態を知った時点から概ね3～5日以内）	報告をしようとする時点において把握している内容
確報	報告対象の事態を知ってから30日以内（不正の目的によるおそれがある漏えい等の場合は60日以内）	全ての報告事項（合理的努力を尽くしても、全ての事項を報告できない場合は、判明次第、報告を追完）

漏えい等報告等の義務化

？ 報告を要しない「高度な暗号化等の秘匿化がされている場合」とは、どのような場合が該当しますか？

当該漏えい等事案が生じた時点の技術水準に照らして、**①漏えい等が発生し、又は発生したおそれがある個人データについて、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられる**とともに、**②そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されている**ことが必要と解されます。

①第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置

適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033等に掲載されている暗号技術が用いられ、それが適切に実装されていること

②暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段の適切な管理

以下のいずれかの要件を満たすこと

- 暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること
- 遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること
- 第三者が復号鍵を行使できないように設計されていること

漏えい等報告等の義務化

？「当該事態の状況に応じて速やかに」本人への通知を行うとは、具体的にどのようなことをいいますか？

速やかに通知を行うことを求めるものですが、**具体的に通知を行う時点**は、個別の事案において、**その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等**を勘案して判断します。

【その時点で通知を行う必要があるとはいえないと考えられる事例（※）】

- 漏えい等のおそれが生じたものの、事案がほとんど判明しておらず、その時点で本人に通知したとしても、本人が必要な措置を講じられる見込みがなく、かえって混乱が生じるおそれがある場合

（※）「当該事態の状況に応じて速やかに」本人への通知を行うべきことに変わりはない。

？本人への通知はどのような事態で行う必要がありますか？

漏えい等報告の義務化されている事態では、本人に対する通知を行う必要があります。

ただし、**本人への通知が困難である場合**には、**代替措置**を講ずることによる対応が認められます。

	考えられる具体例
通知が困難	● 保有する個人データの中に本人の連絡先が含まれていない ● 連絡先が古いために通知を行う時点で本人へ連絡ができない
代替措置	● 事案の公表 ● 問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにする

不適正な方法による利用の禁止

● **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

現　行	改正後
個人情報取扱事業者は個人情報を **適正に取得すべき**ことを法定（§17）	「適正な取得」義務に加えて、 **「不適正な利用」を禁止** ※具体的には、**違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない**旨を法定（§16の2［§19］）

テーマ	法・政令・規則の概要	ガイドライン・Q&Aの概要
②不適正利用の禁止 §16の2 ［§19］	**違法又は不当な行為を助長する等の不適正な方法**により個人情報を利用してはならない旨を明確化する	• **「違法又は不当な行為」**、それを**「助長し、又は誘発するおそれ」**、**不適正な方法による個人情報の利用に該当すると考えられる場合**について、事例を含めて解釈を具体的に記載 ➢ 該当する事例…採用選考を通じて個人情報を取得した事業者が、性別、国籍等の特定の属性のみにより、正当な理由なく本人に対する違法な差別的取扱いを行うために、個人情報を利用 など

不適正な方法による利用の禁止

？「違法又は不当な行為」とはどのような行為をいいますか？

第16条の２［19条］における「違法又は不当な行為」とは、

- **個人情報保護法その他の法令に違反する行為**
- 直ちに違法とは言えないものの、**個人情報保護法その他の法令の制度趣旨や公序良俗に反している等、社会通念上、適正とは認められない行為**

をいいます。

「違法又は不当な行為」の例
暴力団員により行われる暴力的要求行為、本人に対して正当な理由なく行われる違法な差別的取扱い　等

②不適正な方法による利用の禁止

？ 違法又は不当な行為を助長し、又は誘発する「おそれ」とはどのように判断されますか？

第16条の２［19条］における「おそれ」の有無は、個人情報の利用が、違法又は不当な行為を助長又は誘発することについて、**社会通念上蓋然性が認められるか否か**により判断されます。
この判断に当たっては、個人情報の利用方法等の客観的な事情に加えて、個人情報の利用時点における個人情報取扱事業者の認識及び予見可能性も踏まえる必要があります。

「おそれ」が認められると考えられる例：

- 提供先が個人情報を違法に利用していることを認識している等、自己が提供する個人情報についても、同様に違法に利用されることが予見できるにもかかわらず、当該提供先に対して個人情報を提供する場合

「おそれ」が認められないと考えられる例：

- 提供先が個人情報の取得目的を偽っており、当該提供先が取得した個人情報を違法に利用することについて、一般的な注意力をもってしても予見できない状況で、当該提供先に対して個人情報を提供する場合

②不適正な方法による利用の禁止

？ 不適正利用に該当する事例としては、どのようなものが考えられますか？

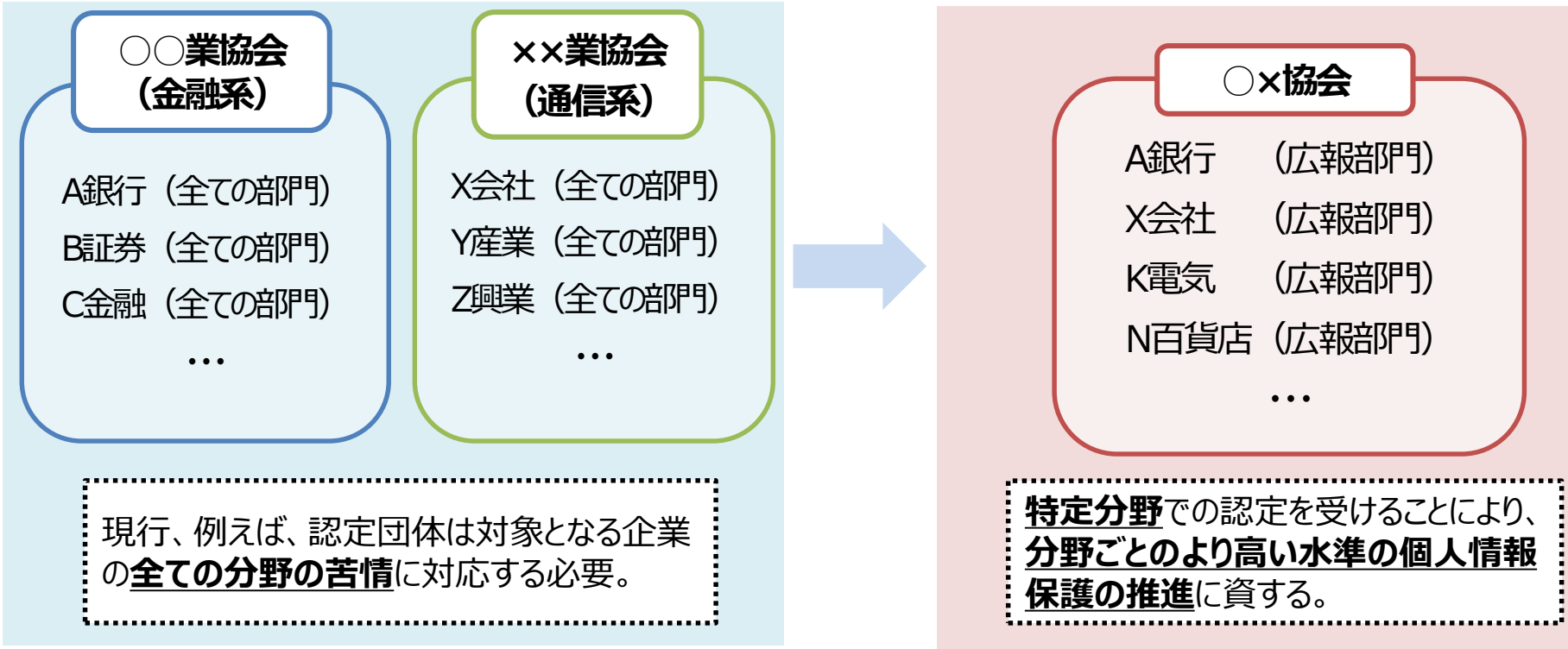
例えば、下記のような、**相当程度悪質なケース**が想定されます。

- 違法な行為を助長するおそれが想定されるにもかかわらず、**違法な行為を営むことが疑われる事業者に対して、個人情報を提供すること**。
- 裁判所による公告等により散在的に公開されている個人情報について、違法な差別が誘発されるおそれがあることが予見できるにもかかわらず、それを**集約してデータベース化し、インターネット上で公開すること**。
- 暴力団員により行われる暴力的要求行為等の不当な行為を助長し、又は誘発するおそれが予見できるにもかかわらず、不当要求による被害を防止するために必要な業務を行う**各事業者の責任者の名簿等を、みだりに開示し、又は暴力団等に対しその存在を明らかにすること**。
- 提供先において第23条［27条］第１項に違反する第三者提供がなされることを予見できるにもかかわらず、当該提供先に対して、**個人情報を提供すること**。
- 性別、国籍等の特定の属性のみにより、正当な理由なく本人に対する**違法な差別的取扱いを行うために、採用選考を通じて取得した個人情報を利用すること**。
- 広告配信を行っている事業者が、違法薬物等の**違法な商品の広告配信のために**、自社で取得した**個人情報を利用すること**。

認定個人情報保護団体制度の充実

● 認定団体制度について、個人情報を用いた業務実態の多様化やIT技術の進展を踏まえ、**企業の特定分野(部門)を対象とする団体を認定できるようにする。**

現　行	改正後
団体を認定し、自主ルールに基づく**企業単位での個人情報全般（企業の全ての分野（部門）が対象）**の適正な取扱いを促す（§47①）	現行制度に加え、**企業の特定分野(部門)を対象**とする団体を認定できるようにする（§47②）



認定個人情報保護団体制度の充実

テーマ	法・政令・規則改正の内容	ガイドライン・Q&Aの概要
①認定個人情報保護団体制度の充実 §47［§47］	現行制度に加え、企業の特定分野（部門）を対象とする団体を認定できるようにする	• 今般の法改正も契機に、**認定団体の望ましい取組の方向性を示すためのガイドライン**を認定団体編として新設 • 制度の目的・意義に加え、①求められる**具体的な業務**（苦情処理、情報提供等）、②**自主ルールの策定**等、③**漏えい等報告**等について記載

① 求められる業務

- 人材の養成・確保を含む**体制を整備して簡易・迅速に苦情に対応**することや、**関係法令や自主ルールの内容等について情報提供**を行うことが求められる。
- 対象事業者が**透明性を確保しながら説明責任を果たすための積極的な指導**や、**PIAの実施や個人データの取扱いに関する責任者の設置などを推奨**することが望ましい。

② 自主ルール（個人情報保護指針）の策定

- **法の内容のみならず**、事業分野等の実態に応じた自主ルールとして、**細目や事例を個人情報保護指針に盛り込む**ことが望ましい。
- 個人関連情報なども含めた各種取組の自主的な実施は、制度趣旨を適切に踏まえた取組。

③ 漏えい等報告

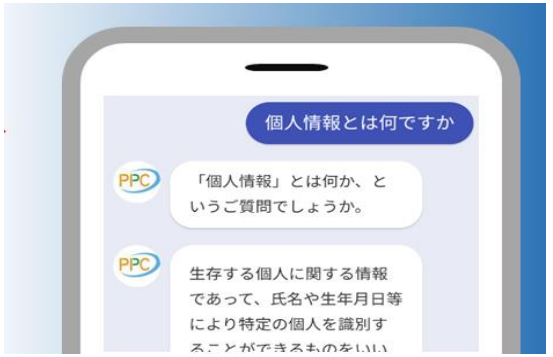
- 自主的取組の一環として、対象事業者から漏えい等事案の情報を受け付けることは有効。
- 事業分野の実態等を踏まえ、必要に応じて、**報告を受け付ける体制を確立し、対象事業者による事案への対応、本人通知・公表等に対する実効的な指導等を行う**ことが望ましい。

個人情報保護委員会へのご相談

●PPC質問チャット

個人情報保護法等に関する皆様からの 質問に対して 24 時間回答できるチャットボットサービス

https://2020chat.ppc.go.jp/



●個人情報保護法相談ダイヤル

個人情報保護法の解釈や個人情報保護制度についての一般的な質問にお答えしたり、個人情報の取扱いに関する苦情の申出についてのあっせんを行うための相談ダイヤル

https://www.ppc.go.jp/personalinfo/pipldial/

電話番号：**03-6457-9849**

受付時間　9:30～17:30（土日祝日及び年末年始を除く）

●PPCビジネスサポートデスク（要予約）

事業者における個人情報の保護及び適正かつ効果的な活用についての啓発の一環として、新技術を用いた新たなビジネスモデル等における個人情報保護法上の留意事項等に関する相談を受付け

https://www.ppc.go.jp/personalinfo/business_support/

電話番号：**03-6457-9771**

受付時間　9:30～17:30（土日祝日及び年末年始を除く）