# 令和2年改正にかかるヒアリング用　チェックリスト

条文番号は令和3年改正に準拠

## 第１　個人情報の把握

１個人情報の棚卸　　（保護対象たる個人情報を正確に把握する必要）

情報のライフサイクル（取得、保管、利用、提供、廃棄）の確認

取得時の利用目的の告知は明確になされているか

本人の同意を確認したか

保有個人情報の洩れのチェック

開示対象となる情報群（通常の顧客情報など）は、整理され、網羅されているか

保有個人情報以外の個人情報群の点検

（開示対象とならないブラック情報など）　　漏洩したり、既存した場合の対応が必要

保有個人情報以外の特別な情報群を確認しているか、安全に保管されているか

２個人情報の最新性・正確性確認　（漏洩等の連絡など確実に連絡できることを担保）

すべての本人に確実に連絡がとれるか

３ **（新設）個人情報関連情報**の存否、取り扱い

個人関連情報とは識別できない「ある人」に関する情報（個人情報の一部）であって、統計情報などもともと個人情報に該当しない情報とは区別される情報群をいう。個人関連の匿名情報に該当する（匿名加工しない、元々の匿名情報）。

個人関連情報の存否　　①クッキー情報　②アクセスログ　③閲覧履歴　④ある人の年齢、性別など

顧客等の動向分析等の確認のため、多様な情報を取得している場合に、該当情報の有無が問題となる

個人関連情報を取得し、利用しているか

利用方法の確認

利用することを本人に説明しているか

個人関連情報の第三者提供の制限

クッキー情報やアクセスログ情報を関連事業者、下請け事業者から取得している

第三者提供にかかる本人同意が必要　§26　1項　情報収集の段階での包括同意

本人同意の確認方法が確立され、実施されているか

提供記録、取得記録はされているか

４（新設）仮名加工情報

仮名加工情報（個人情報の一部を削除等した情報）の存否　　ある場合の取扱状況は明確か

仮名加加工情報がある場合の公表義務を果たす体制はできているか　§40

（1）個人情報である仮名加工情報（識別情報が保有されている場合）たる個人データ

個人情報にかかる制限（目的制限等　＋注意義務）がすべて適用になる

（２）個人情報ではない仮名加工情報（識別情報が消去されている場合）

個人情報ではないが、元が個人情報であった経緯から、各種注意義務はある

第三者提供禁止　（例外は法令の場合のみ）であることを理解しているか、関連会社に提供していないか

例外　①委託　②事業承継　③共同利用　　などがあるか

５外国人情報の存否

（１）国内での外国人情報の取扱いの有無　　取扱状況を把握しているか

（２）海外での外国人情報の取扱いの有無　　取扱状況を把握しているか

（３）海外の外国人の個人情報について国内移転の有無　　取扱状況を把握しているか

６ **（新設）不適正利用の禁止**　§19

違法又は不当な行為を助長し、誘発するおそれのある方法での利用を禁止しているか

（１）官報情報利用があるか

（２）裁判所情報利用があるか

（３）暴力団・総会屋情報の利用があるか

（４）応募情報の不適切利用があるか、目的外利用があるか

（３）違法薬物、違法物品販売等に個人情報を利用してメールなどすることがないか

７ **（新設）漏洩報告・本人通知**　§２６

報告原因　意図に反して

追加　　意図に反する廃棄の場合に、報告、通知をしているか

意図に反する毀損（復元キー喪失、暗号化され使えないなど）の場合に通知、報告しているか

ウイルス感染により使用できなくなった場合や、サーバに対する不正アクセスで窃取された痕跡がある場合などに、通知、報告しているか

報告体制　委託先は委託元へ報告を行っているか、委託元は認識しているか
管理者は個情委へ報告を行っているか、管理者は認識しているか
第一報は、知ってから3～5日以内
覚知後30日、または60日以内に確定報告が必要（ただし、追完も可能）
本人通知体制の確立、システムの修正など、さらには見直し、更新などはされているか

## 第２　保有個人情報の利用目的の点検

1年以内、6か月以内のデータを別枠としていないか　**（R2改正ですべて保有個人データとなった）**

1 保管部署での使用目的は網羅されていることを確認したか

2 新たな利用目的が発生していないか

3 新たな利用目的があった場合の対応策を理解しているか

4 **（新設）保有個人情報に対する安全管理措置の内容の「知りうる状態」の確立が確保されているか**
法32条、政令10条１項3号④　追記
公表（知りうる状態）内容：物理的、技術的、組織的、人的安全管理措置の内容の説明
本人からの問合せがあった場合の回答が、迅速に行われる体制ができているか
（なお、個人情報自体の安全管理措置について公表があれば、それに代えることができる）

## 第３　権利保護対応

大前提　個人情報の一元化ができているか
本人からの指定がなされた場合、当該本人の全個人情報を利用停止にできるか

1 利用停止請求
**（新設）　必要がない場合、正当な権利が侵害されるおそれがある場合の利用停止請求　§34　Ⅴ**
**本人から利用停止要求がなされた場合に、すべてを利用停止とできる体制があるか**

2 開示請求
**（新設）デジタルデータでの提供が可能な体制があるか**
**（新設）第三者提供記録についての開示　関連会社などへの提供などを開示できるようにしているか**

3 訂正請求

## 第４　第三者提供の実態

1 **（新設）第三者提供記録の開示　§33　5項　　開示義務（デジタルデータを含む）**　同上
2 **（新設）不正取得された個人データ、オプトアウトにより提供されたデータについて、**
**オプトアウトでの第三者提供を禁止しているか**
3 子会社への移転状況についての確認は行われているか
4 関連会社への移転状況についての確認は行われているか
5 共同利用状況についての確認は行われているか
6 提供記録・受領記録をとっているか、確認は行われているか

## 第５　安全管理措置対応**（保有個人データの安全管理措置の新設　前記第２・４に連動）**

1 基本方針の策定について

（1）個人データの適正な取扱いの確保のため、「関係法令・ガイドライン等の遵守」、「質問及び苦情処理の窓口」等についての基本方針を策定し、公開しているか

（2）取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について個人データの取扱規程を策定し、公開しているか

2 技術的安全管理措置の実施状況
（1）アクセス制御を実施して、担当者及び取り扱う個人情報データベース等の範囲を限定などして、適切なアクセス制御を行なっているか　（ガイドライン）

（2）外部からの不正アクセス、不正ソフトなどからの攻撃を防止する措置をとっているか　（ガイドライン）

3 物理的安全管理措置の実施状況
（1）個人データを取り扱う区域において、従業者の入退室管理及び持ち込む機器等の制限を行うとともに、権限を有しない者による個人データの閲覧を防止する措置を実施などの措置を実施しているか　（ガイドライン）

（２）個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を講じるとともに、事業所内の移動を含め、当該機器、電子媒体等を持ち運ぶ場合、容易に個人データが判明しないよう措置を実施などの求められる措置を実施しているか　（ガイドライン）

4 組織的安全管理措置の実施状況

（１）個人データの取扱いに関する責任者を設置するとともに、個人データを取り扱う従業者及び当該従業者が取り扱う個人データの範囲を明確化し、法や取扱規程に違反している事実又は兆候を把握した場合の責任者への報告連絡体制を整備するなどの対応をしているか　（ガイドライン）

（２）個人データの取扱状況について、定期的に自己点検を実施するとともに、他部署や外部の者による監査を実施するなどの監査体制を確立しているか　（ガイドライン）

5 人的安全管理措置の実施状況

（１）個人データの取扱いに関する留意事項について、従業者に定期的な研修を実施するなどして、従業者の遵守体制を確保しているか　（ガイドライン）

（２）個人データについての秘密保持に関する事項を就業規則に記載するなどして、守るべき指針を明示しているか　（ガイドライン）

6 外的環境の把握

個人データを保管しているA 国における個人情報の保護に関する制度を把握した上で安全管理措置を実施しているか　（ガイドライン）