

個人情報保護上の重要チェックポイント

※個人情報保護のために社内検討や弁護士相談する際に主に検討すべき事項を簡易的にまとめたもの

※ミス・漏れ等もあるため、使用する際は再度の確認が必要。また必ず法律本文、ガイドライン本文に当たっていただくようお願いします。

※Copyright © 弁護士水町雅子 All Rights Reserved. (無断転用等禁止)

※気が向いたら更新して充実させていきます。

ポイント	内容
I 基本情報	
1. 業務の全体像・目的	
2. 登場人物	自社以外にどのような関係者が関わるか
3. 個人情報の内容	どのような個人情報を取り扱うのか
4. 要配慮個人情報やプライバシー性の高い情報を含むか	
5. 個人情報の本人（対象者）の範囲・数	誰の個人情報を取り扱うのか。概数は。
6. これらの個人情報を取り扱う理由	
II 個人情報の入手	
1. 入手元	
2. 入手方法	
3. 法的根拠	
4. 本人の予測可能性	
5. 目的外の入手が行われるリスク（必要な対象者以外、必要な内容以外の入手が行われるリスク）への対策	個人情報を過剰取得しないようにする対策
6. 入手した個人情報が不正確であるリスクへの対策	対象者間違い、内容の不正確性を排除するための対策 情報が不正確なことによる悪影響（対自社、本人、外部等）
7. 入手の際に個人情報が漏えい・紛失するリスクへの対策	
8. 入手に際する確認はどのように履践したか	個人情報保護法26条
8. その他、留意すべき事項はないか	
III 個人情報の利用	
1. 利用目的（プライバシーポリシー等で特定しているもの）は何で、どのように公表・通知・明示されているか	
2. 利用方法（詳細）	

3. 利用目的は十分特定されていて、今回の利用は利用目的の範囲内といえるか	
4. 利用の主体（使用部署、使用者数）	
5. 情報の突合をするか、情報の分析をするか、本人にどのような影響を与え得るか	
6. 本人の予測可能性	
7. 目的を超えた紐付けが行われるリスクへの対策	過剰な紐づけ、過剰利用がなされないようにするための対策
8. 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスクへの対策	個人情報が無関係の者に利用されないように ユーザ認証、アクセス権限の発効・執行管理、アクセス権限の管理、使用記録
9. 違法な目的外利用がなされるリスクへの対策	
10. 個人情報が不正に複製されるリスクへの対策	
11. その他、留意すべき事項はないか	
IV 個人情報の委託	
1. 委託の有無	
①委託内容	
②委託する個人情報の範囲、本人の範囲、本人数	
③委託先における取扱者数	
④委託先への個人情報の提供方法	
⑤委託先選定にあたって、委託先の適正性の確認方法	
情報保護管理体制の確認	
個人情報の閲覧者・更新者の制限	
個人情報の取扱いの記録	
個人情報の提供ルール	
委託先から他者への提供に関するルール内容及びルール遵守の確認方法	
委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法	
個人情報の消去ルール	
その他	
⑥委託契約の適正性の確認方法	
⑦契約後も継続的に委託先を監督する方法	
2. 再委託の有無	
①再委託の許諾方法	
②再委託内容	

③再委託する個人情報の範囲、本人の範囲、本人数	
④再委託先における取扱者数	
⑤再委託先への個人情報の提供方法	
⑥再委託先選定にあたって、再委託先の適正性の確認方法	
⑦再委託契約の適正性の確認方法	
⑧再委託先を監督する方法	
3. 再々委託以降の有無等	
4. その他、留意すべき事項はないか	
IV 個人情報の提供	
1. 提供の有無	
①法的根拠・妥当性	
②提供先における利用目的	
③提供する情報	
④提供する情報の対象となる 本人の範囲・数	
⑤提供方法	
⑥外国提供の有無、有の場合の国名・法的根拠	個人情報保護法 24 条
⑦時期・頻度	
⑧提供先がさらに提供するか、する場合の適正性の確認方法	
⑨本人の予測可能性	
⑩不正な提供が行われるリスクへの対策	提供記録、ルール、権限等
⑪不適切な方法で提供が行われるリスクへの対策	
⑫誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスクへの対策	
⑬提供記録の有無	個人情報保護法 25 条
2. その他、留意すべき事項はないか	
IV 個人情報の保管・消去	
1. 保管の有無	
①保管場所	
②保管期間	
③消去方法	
2. 個人情報の漏えい・滅失・毀損リスクへの対策	

①NISC政府機関統一基準群その他適用しているルール	
②安全管理体制	
③安全管理規程	
④安全管理体制・規程の職員への周知	
⑤物理的対策	
⑥技術的対策	
⑦バックアップ	
⑧事故発生時手順の策定・周知	
⑨過去に個人情報に関する重大事故が発生したか	
⑩死者の個人情報の保管方法	
3. 個人情報が古い情報のまま保管され続けるリスクへの対策	
4. 個人情報が消去されずいつまでも存在するリスクへの対策	
5. その他、留意すべき事項はないか	
V その他のリスク対策	
1. 監督	
従業者の監督はどのように行っているか	
2. 監査	
①自己点検	
②監査（内部／外部）	
③監査結果の活用をどのように行っているか	
3. 従業者に対する教育・啓発	
4. 匿名加工情報の有無・対応	
5. その他、留意すべき事項はないか	
VI 開示請求、問合せ	
1. 個人情報の開示・訂正・利用停止請求	
①請求先	
②請求方法	
③手数料	
④対応方法は整備されているか、正しく対応できているか	
⑤苦情等は来ていないか	
2. 個人情報の取扱いに関する問合せ	

①連絡先	
②対応方法は整備されているか、正しく対応できているか	
③苦情等は来ていないか	
④改善事項はないか	